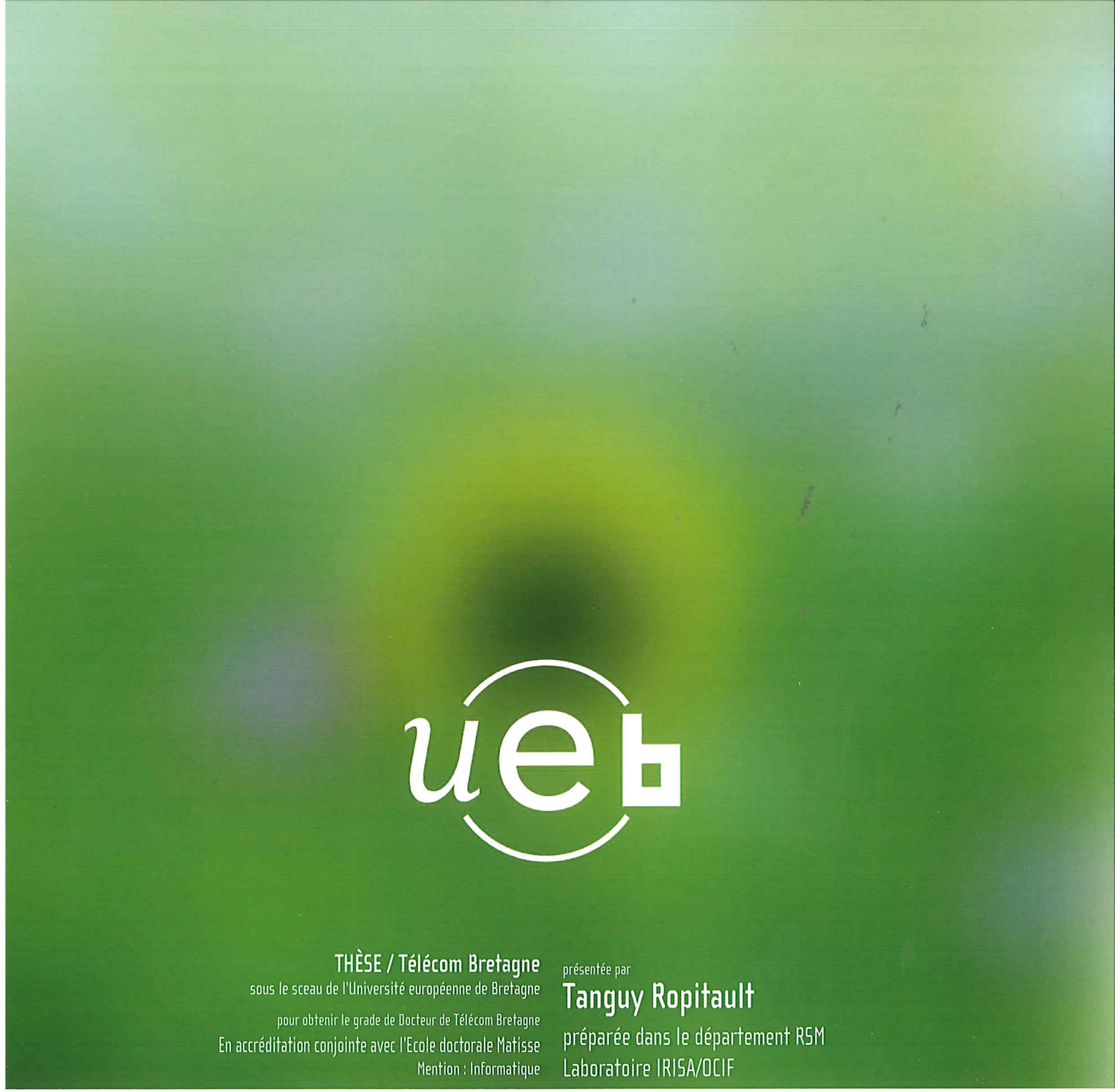
Routage et performances dans les réseaux CPL pour le Smart Grid

Tanguy Ropitault



THÈSE / Télécom Bretagne
sous le sceau de l'Université européenne de Bretagne

pour obtenir le grade de Docteur de Télécom Bretagne
En accréditation conjointe avec l'Ecole doctorale Matisse
Mention : Informatique

présentée par
Tanguy Ropitault
préparée dans le département RSM
Laboratoire IRISA/OCIF

Routage et Performances dans les réseaux CPL pour le Smart Grid

Thèse soutenue le 18 juin 2015
Devant le jury composé de :

César Viho
Professeur, Inria - Université de Rennes 1 / président

Pascale Minet
Chargée de recheche (HDR), Inria Paris-Rocquencourt / rapporteur

Thomas Noel
Professeur, Université de Strasbourg / rapporteur

Laurent Toutain
Maître de conférences (HDR), Télécom Bretagne / directeur de thèse

N° d'ordre : 2015telb0360

Sous le sceau de l'Université européenne de Bretagne

Télécom Bretagne

En accréditation conjointe avec l'Ecole Doctorale Matisse

Ecole Doctorale – MATISSE

Routage et Performances dans les réseaux CPL pour le Smart Grid

---

Thèse de Doctorat

Mention : Informatique

Présentée par **Tanguy Ropitault**

Département : RSM

Laboratoire : IRISA/OCIF

Directeur de thèse : Laurent TOUTAIN

Soutenue le 18 Juin 2015

Jury :

Mme Pascale Minet, Chercheur, INRIA Paris Rocquencourt (Rapporteur)
M. Thomas Noël, Professeur, Université de Strasbourg (Rapporteur)
M. Laurent Toutain, Enseignant Chercheur, Telecom Bretagne (Directeur de thèse)
M. Alexander Pelov, Enseignant Chercheur, Telecom Bretagne (Encadrant)
Mme Yvonne-Anne Pignolet, Principal Scientist, ABB (Examinateur)
M. César Viho, Professeur, Université de Rennes 1 (Examinateur)
M. Philippe Chiummiento, ITRON (Invité)
M. Dominique Poissonnier, Texas Instruments (Invité)

To my family.

Acknowledgments

I would like to thank Dr. Alexander Pelov and Dr. Laurent Toutain for guiding me for my thesis. Your precious advices helped me all along the life of this thesis. I did not only meet fount of knowledge, very wisdom and passionated researchers, but also great persons, always looking for helping me to give the best of me. I would thank you all my life.

I would also like to thank Prof. Xavier Lagrange for his precious guidance about the physical part of this thesis. I would also want to thank Prof. Pascale Minet, Prof. Thomas Noël, Dr. Yvonne-Anne Pignolet, Philippe Chiummiento and Dominique Poissonnier for accepting to be part of my jury and for their insightful questions and comments.

My acknowledgments go also to the companies ITRON and Texas Instrument for funding this thesis and their helps for understanding the research regarding to industrial perspectives. I am going to miss those insightful discussions specially with Philippe Chiummiento and Ramanuja Vedantham.

A special thanks to the Hudson Soft company for having created my favorite source of relaxation all along that thesis: Super Bomberman.

I would like also to thank all the person in Telecom Bretagne that I met across all these years. A very special thank to my Argentinian colleagues, Alejandro and Renzo, I stil don't speak spanish, but I know the important words. A special thank also to Nicolas, who hired me in Telecom Bretagne. Without you, I would not be there now. You were the first one to believe in me. In my turn to admit that I believe in you, and that one day, you may beat me to badminton. I would also like to thank Tanguy, Fabien, Baptiste, Benjamin, Manu, Benoit, Lucien, Sara, Anais, and Marie-Pierre, for all the moments of fun we shared together.

At last but not least, I would like to thank the one that makes it happen. Thanks you Samantha, for your love, your advices, your help. Thank you for being the one you are. May life together be bright and forever.

Abstract

The power grid has begun a major evolution in the past decade, laying the foundations of what is known as the Smart Grid. The Smart Grid relies on bidirectional communications in order to enable new functionalities such as efficient management of production and distribution of electricity, real-time pricing information and consumption feedback to end-users, integration of renewable energy sources and electrical vehicles, and demand response.

One of the key components of the Smart Grid is the Advanced Metering Infrastructure that enables the interconnection between users and utilities thanks to a new generation of power meters: the Smart Meter. While Smart Meter deployments have already started worldwide at the instigation of governments, a multitude of choices still remains to be done concerning their technical implementations.

Specifically, Smart Meter networking can be based on Power Line Communication (*PLC*), which is one of the major networking technologies available to utilities. P1901.2, a narrowband PLC has been standardized by the IEEE for usage in the Smart Grid. However, debates are still open for the routing protocol to use for these new high-density, narrowband PLC networks. PLC, being a harsh environment (low bandwidth, noisy, etc.), has most of the characteristics of a Low power and Lossy Network. As a result, the protocol RPL, designed specifically for Low power and Lossy Network, is a prime candidate for routing in IEEE P1901.2 networks.

The goal of this thesis is to study RPL's behavior in Smart Grid environment and to provide adjustments to its behavior in order to improve the network performance in a narrowband PLC network of Smart Meters.

For that purpose, we implemented a complete IEEE P1901.2 simulation environment (from physical to applicative layer) in the simulator OPNET, which we validated against a real-world testbed.

Then, we proposed a new way to manage the routing process during RPL's startup phase. By adapting a specific RPL message emission policy which depends on the network conditions, we ensure a faster creation of the routing topology.

As PLC traffic patterns are different from the ones initially considered for the design of RPL, we introduced a new mechanism to handle link-breakage and non-working Smart Meters. This mechanism, using a slightly modified version of Neighbor Unreachability Detection, allows faster detection and reaction to link-breakage.

Finally, we proposed a new RPL metric that allows to overcome ETX's main drawbacks and that can fully benefit of the multi-modulation scheme of IEEE P1901.2 standard.

Resumé

Le réseau électrique a connu récemment une évolution majeure et s'est transformé en un réseau électrique intelligent : le Smart Grid. La bidirectionnalité est au cœur du Smart Grid et permet de mettre en œuvre et de prendre en compte un ensemble de nouvelles fonctionnalités telles que : la gestion efficace de la production et de la distribution d'électricité, l'obtention d'informations temps-réel sur la consommation et le tarifage de l'électricité pour l'utilisateur, l'intégration des énergies renouvelables et des véhicules électriques dans le réseau, et une réponse temps-réel réagissant à la demande afin de réduire les pics de consommation.

Un des éléments majeurs du Smart Grid est l'Advanced Metering Infrastructure qui permet d'assurer l'interconnexion entre utilisateurs et opérateurs énergétiques à l'aide d'une nouvelle génération de compteur : "les compteurs intelligents". Alors que le déploiement de compteur intelligent a déjà commencé dans le monde sous l'instigation des différents gouvernements, une multitude de choix reste encore à faire concernant leur mise-en-œuvre.

Concernant le medium de communication, le Courant Porteur en Ligne (CPL), utilisant les lignes électriques déjà déployées, semble être la solution idéale pour les opérateurs énergétiques. Le standard P901.2 a été standardisé par l'IEEE pour permettre des communication efficaces au sein du Smart Grid. Il préconise l'utilisation du protocole IPv6 mais ne donne aucune indication concernant le protocole de routage à utiliser. Le CPL est un environnement extrême de part sa nature (bruits, faibles débits) et peut-être vu comme un Low Power and Lossy Network (LLN) (réseaux à faible puissance et fort taux de perte en Français). Le groupe de travail ROLL a défini le protocole pro-actif RPL spécifiquement pour les LLN et semble, de ce fait, un bon candidat pour les environnements IEEE P1901.2.

Le but de cette thèse est d'étudier le comportement de RPL dans le Smart Grid et d'apporter des améliorations spécifiques pour le Smart Grid afin de garantir un fonctionnement optimal de RPL dans ce type d'environnement.

Dans cette optique, nous avons implémenté par simulation un environnement IEEE P1901.2 complet, de la modélisation du canal physique jusqu'au couche applicative. Nous avons validé ce simulateur en le comparant à une plateforme réelle.

Nous avons ensuite proposé un nouveau moyen de gérer la création de route durant la phase de démarrage de RPL. En adaptant spécifiquement les temporisations gérant l'émission de messages RPL, nous garantissons une formation de la topologie de routage plus rapide en prenant en compte l'importance des communications de l'opérateur électrique vers les compteurs intelligents.

Les types de trafic générés au sein du Smart Grid étant différents de ceux ayant

conduit à l'élaboration de RPL, nous avons mis en œuvre un nouveau mécanisme pour gérer les liens (ou compteurs intelligents) défaillants. Cette solution utilise une version légèrement modifiée de Neighbor Unreachability Detection qui permet une détection et une réaction plus rapide en cas de lien ou de compteur intelligent non-fonctionnels.

Enfin, nous avons défini une nouvelle métrique pour RPL qui permet de s'affranchir des problèmes liés à la métrique ETX. Cette métrique, appelée Channel Occupancy, permet de prendre en compte les environnements utilisant un schéma de modulations multiple dans le but de minimiser le temps d'occupation du canal physique.

Resumé en français

Depuis que l'Homme a réussi à appréhender l'électricité, les moyens de production et de distribution de celle-ci ont constamment évolué. Le changement majeur opéré au cours des dernières décennies a été d'intégrer les technologies de l'internet dans le réseau électrique afin de transformer le réseau électrique en un «réseau électrique intelligent». Aujourd'hui, le réseau électrique doit surmonter de nouveaux défis et faire face à de nouvelles contraintes comme :

- Gérer efficacement la production et de la distribution du courant ;
- Fournir des retours aux utilisateurs à propos de de la tarification et de la consommation ;
- Intégrer dans le réseau les énergies renouvelables ;
- Prendre en compte l'apparition des véhicules électriques ;
- Penser à une nouvelle gestion de l'offre et de la demande afin de faire diminuer les pics de charge ;
- Faire face à l'apparition des micros-sources locales de génération de courant.

Du point de vue de la distribution, les anciennes générations de réseau électrique permettaient une collecte d'information très limitées (lecture des kWh consommés ou analyse des pics de consommations pour un mois) et ceci d'une manière unidirectionnelle. Le nouveau réseau électrique a besoin d'avoir une connaissance précise et temps-réel de la consommation d'énergie et ceci à tous les endroits du réseau, et en plus de pouvoir communiquer de manière bidirectionnelle avec tous les éléments du réseau – l'essence même du réseau électrique intelligent.

Deux principaux domaines peuvent être distingués dans le réseau électrique actuel : le domaine « opéré » en charge de la génération, de la transmission, et de la distribution d'électricité, et le domaine « consommateur ». La frontière séparant ces deux domaines est de la plus haute-importance notamment pour la facturation, mais plus récemment pour des fonctionnalités plus perfectionnées comme par exemple :

- La gestion de la demande comme arrêter la climatisation pour quelques minutes lors d'un pic de charge ;
- Le contrôle d'un flux d'énergie bidirectionnelle comme par exemple un consommateur qui a un moyen de produire de l'énergie et qui l'injecte dans le réseau.

Cette bordure entre domaine «opéré» et «consommateur » est la plupart du temps matérialisé par le compteur électrique. Obtenir un canal de communication bidirectionnelle à l'aide d'un compteur électrique informatisé (le « compteur intelligent ») est donc un des éléments essentiels du réseau électrique intelligent.

Dans certains cas, le compteur électrique intelligent peut être directement joint par l'opérateur énergétique en utilisant une technologie «WAN» (Wireless Area Network en anglais) existante (par exemple le réseau cellulaire classique). Cependant, une multitude de facteurs empêche souvent une communication directe et impose de facto l'utilisation de réseaux locaux dédiés (Les «NAN» pour Neighbor Area Network en anglais) qui connectent les compteurs à proximité comme ceux d'un quartier ou ceux connectés au même transformateur électrique.

Le système englobant les compteurs intelligents, les réseaux nécessaires à leur communication (WAN et NAN), et le système de gestion est appelé «AMI» (pour Advanced Metering Infrastructure en anglais). L'AMI repose sur des NAN robustes et efficaces pour transporter l'information entre les compteurs électriques intelligents et les concentrateurs de données. Les concentrateurs de données sont les éléments connectant les LAN et les WAN et peuvent varier en complexité : d'un simple répéteur à une passerelle applicative complète. Dans de la cadre de cette thèse, nous nous focalisons sur l'environnement AMI et plus spécifiquement sur les communications entre les concentrateurs de données et les compteurs électriques intelligents.

L'AMI est un élément clé du réseau électrique intelligent et permet de surveiller en temps-réel la consommation électrique, permettant de ce fait à l'opérateur énergétique d'agir et de réagir à l'évolution du système. Au moment de la rédaction, il y a environ 45 millions de compteurs électrique intelligent déjà installés par trois pays européens (la Finlande, l'Italie et la Suède). La Commission Européenne a recommandé que 200 millions de compteur électrique intelligent soient déployés d'ici à 2020 (représentant environ un taux d'équipement de 72% du parc européen de compteur). Malgré les récents efforts fournis pour définir l'architecture du réseau électrique intelligent et le fait que le déploiement des compteurs électriques intelligent ait déjà commencé à l'échelle mondiale, le réseau électrique intelligent est aujourd'hui plus une vision qu'une réalité et beaucoup de choix restent encore à faire par les opérateurs énergétiques et le marché comme de choisir :

- Le medium physique de communication (sans-fil ou filaire) c'est-à-dire le medium utilisé pour transporter les données ;
- Les protocoles réseaux nécessaires à la transmission et au routage du trafic entre les compteurs intelligents et les opérateurs énergétiques.

Concernant le medium physique, deux principales options sont disponibles : un environnement filaire ou sans-fil. Une des solutions les plus prometteuses pour transporter les données au sein du réseau électrique est une solution filaire : le « CPL » (pour Courant Porteur en Ligne). Le CPL permet de transporter les données sur les lignes électriques et offre le gros avantage, comparé aux solutions sans-fil, d'un coût de déploiement limité vu que les lignes électriques sont déjà existantes. Par conséquent, le CPL a été choisi par les opérateurs énergétiques et l'industrie des compteurs intelligents comme un candidat potentiel pour le medium physique. Cependant, à cause de ses caractéristiques intrinsèques extrêmes (environnement bruité, faible dé-

bit, etc.), l'utilisation du CPL dans les réseaux électriques intelligents représente différents challenges qui doivent être résolus à l'aide de solutions CPL spécifiques. A cette fin, une grande partie des industriels et des experts mondiaux ont défini le protocole « P1901.2 » qui a été standardisé à l'IETF. Ce protocole utilise des fréquences à bande étroite (<500kHz) qui peuvent offrir un débit jusqu'à 500kbps en fonction de la régulation en vigueur. Notre thèse étudie le protocole IEEE P1901.2 plus particulièrement pour la bande CENELEC A, c'est-à-dire la bande réservée pour les opérateurs énergétiques en Europe. Le choix du medium physique de communication n'est pas le seul choix devant être fait par les opérateurs énergétique : le choix des protocoles réseaux de communication est de la plus haute importance. IEEE P1901.2 impose l'utilisation d'IPv6. Les motivations pour choisir une solution purement IP sont basées sur le succès d'IP comme couche de convergence (plus de deux milliards de personnes utilisent l'internet quotidiennement) et aussi sur son ancienneté (plus de 30 années de développement et d'amélioration) qui facilitent des standards ouverts et interopérables. Le protocole IPv6, apportant de nombreuses améliorations au protocole IPv4 (autoconfiguration facilitée, un espace d'adressage plus grand, etc.) est la solution idéale pour les nouveaux réseaux et a donc été choisie par les opérateurs énergétiques pour le développement de réseaux intelligents.

Alors qu'IPv6 a été largement adopté comme un élément clé du réseau électrique intelligent, les débats sont toujours en cours concernant le protocole de routage à utiliser. Le CPL, avec ses caractéristiques, peut être vu comme un réseau à faible puissance et fort taux de perte («LLN» en anglais pour Low power and Lossy Network) c'est-à-dire un réseau composé d'appareils fortement contraints. Le groupe de travail ROLL de l'IETF a défini un protocole spécifiquement pour les LLN. Ce protocole, «RPL», permet de construire et d'installer des topologies de routage sans boucle grâce à une structure appelé DAG, centrées sur une seule destination : le puits de données. Cela permet d'avoir des routes bidirectionnelles depuis les capteurs jusqu'au puits de données (des compteurs intelligents au concentrateur de données dans l'environnement AMI) ce qui sied totalement au premier objectif du réseau électrique intelligent : la bidirectionnalité des communications. RPL a été principalement créé de façon à optimiser le trafic MultiPoint-a-Point (même si il permet le trafic Point-a-Point et Point-a-Multipoint), et cherche plus particulièrement à optimiser les routes des capteurs au puits de données ; Jusqu'à présent, les performances du protocole de routage RPL ont été étudiées dans la littérature dans le contexte des réseaux sans-fil. Ainsi, peu de résultats sont disponibles dans les environnements CPL et encore moins dans les architectures AMI. Les motifs de trafic ont été identifiés et catégorisés en deux parties :

- Des compteurs intelligents au point terminal de la communication («M2HE» pour Meter to Head-End en anglais)
- Du point terminal de communication aux compteurs intelligents. (“HE2M” pour Head-End to Meter en anglais)

Le trafic HE2M a une importance capitale car il permet à l'opérateur énergétique de communiquer avec les compteurs intelligents en fonction des évènements (par exemple stopper des équipements, déclencher des lectures spontanées de compteurs, ou mettre à jour le micrologiciel des compteurs). RPL doit donc être étudié dans les environnements AMI PLC pour analyser son efficacité et ceci quel que soit le type de trafic (M2HE ou HE2M) afin de déterminer si des optimisations spécifiquement adaptées aux AMI sont nécessaires.

Pour étudier les performances de RPL, nous avons architecturé et implémenté un simulateur IEEE P1901.2 complet en utilisant le simulateur OPNET. Cette phase a consisté à proposer et à mettre en œuvre un modèle de canal physique P1901.2, et aussi le développement complet du protocole P1901.2. En plus du protocole de routage RPL, nous avons implémenté les protocoles de routage LOAD et LOADng afin d'avoir une base de comparaison. En effet, LOAD et son évolution LOADng, ont été choisis comme protocole de routage par défaut pour le protocole « G3-PLC », un autre standard PLC pour les fréquences à bande étroite définit spécifiquement pour les réseaux électrique intelligent. Pour évaluer la technologie CPL, l'industrie des AMI se repose sur des métriques observées à large-échelle (1500 nœuds par concentrateur de données), avec une large base de topologies (rurale, urbaine, ou mixte) et sur différents profils de bruits et d'impédances. Les évaluations sur le terrain sont généralement limitées à un faible nombre de nœuds, de topologies, et de profils. La principale limitation provient d'un problème de coût associé au déploiement de pilotes de test. La seule alternative viable au déploiement terrain est la simulation. Nos résultats de simulations ont été comparés et validés avec des résultats obtenus sur le terrain afin de garantir la qualité de la mise en œuvre de l'implémentation dans le simulateur.

La contribution principale de notre thèse est de proposer des adaptations et des optimisations au protocole RPL spécifiquement adaptées à l'environnement P1901.2 AMI. Les améliorations proposées peuvent se classifier en deux catégories :

- Formation des routes : Le processus consistant à créer des routes bidirectionnelles entre les compteurs intelligents et le concentrateur de données durant le démarrage du réseau ;
- Gestion des routes : La phase pendant laquelle RPL atteint son état stationnaire et où les routes doivent être maintenues et mises à jour selon les conditions du réseau (qualité du lien qui change, lien qui casse, ou compteur intelligent non-opérationnel).

Notre objectif est de minimiser le surplus de signalisation, le temps de convergence, le temps de réparation dans le cas d'un lien non-fonctionnel, et le délai de bout-en-bout, tout en maximisant le taux de transmission. Nous proposons une approche distribuée (4Dia) pour améliorer le temps de convergence durant la phase de formation des routes. Cette méthode calcule dynamiquement l'émission des messages de signalisation en fonction des conditions du réseau, et ceci afin d'éviter les

congestions et d'accélérer le processus de formation des routes. Nous introduisons aussi une nouvelle définition du temps de convergence pour les environnements AMI en soulignant le fait que la bidirectionnalité des communications entraine des nouvelles exigences. De ce fait, le temps de route formation doit non seulement prendre en compte le temps pour former les routes descendantes mais aussi le temps de formation des routes montantes, contrairement à ce qui est définit dans la littérature où seul le temps pour former les routes descendantes est pris en compte.

Nous améliorons la gestion des routes en ajoutant une nouvelle méthode pour réagir au cassure de lien ou au lien non-fonctionnel : FRLD. Ce mécanisme est basé sur une version légèrement modifiée de NUD. Il permet d'accélérer la réaction au lien non-fonctionnel ainsi que de procéder à l'installation des routes nécessaires pour une réaction rapide. Nous réduisons aussi le surplus de signalisation en ajoutant un nouveau critère pour gérer l'émission des messages DAO en fonction du retour de l'opérateur énergétique. Finalement, nous avons introduit une nouvelle métrique pour RPL : Channel Occupancy. Cette métrique cherche à minimiser l'occupation globale du canal en calculant le cout du chemin en fonction de la modulation utilisable pour chaque lien. Ainsi, les routes sont construites en minimisant l'occupation du canal. Contrairement à la métrique ETX, Channel Occupancy tend à utiliser plus de saut pour transmettre les données mais permet de réduire le délai de bout en bout et de maximiser le taux de transmission des données.

List of Publications

International Conferences

T. Ropitault, A. Lampropulos, A. Pelov, L. Toutain, R. Vedantham, and P. Chiummiento. *Realistic model for narrowband PLC for advances metering infrastructure*, In IEEE International Conference Smart Grid Communications (SmartGridComm), 2013.

T. Ropitault, A. Lampropulos, A. Pelov, L. Toutain, R. Vedantham, and P. Chiummiento. *Doing it right 2014; recommendations for RPL in PLC-based networks for the smart grid*, In IEEE International Conference Smart Grid Communications (SmartGridComm), 2014.

T. Ropitault, A. Lampropulos, A. Pelov, L. Toutain, R. Vedantham, and P. Chiummiento. *Optimizing PLC Networks for the Smart Grid with a new multi-modulation RPL metric – Channel Occupancy*, submitted to IEEE International Conference Smart Grid Communications (SmartGridComm), 2015.

T. Hartmann, F. Fouquet, J. Klein, Y. Le Traon, A. Pelov, L. Toutain, T. Ropitault. *Generating realistic Smart Grid communication topologies based on real-data*, In IEEE International Conference Smart Grid Communications (SmartGridComm), 2014.

Acronyms

4Dia Distributed Dynamic DelayDAO interval adjustment
6LoWPAN IPv6 over Low power Wireless Personal Area Networks
ADRM Aggressive Downward Route Management
ADTL Average Data Transmission Level
AMI Advanced Metering Infrastructure
AODV Ad Hoc On-Demand Distance Vector Protocol
APTL Average Preamble Transmission Level
ARIB Association of Radio Industries and Businesses
ASTL Average Sub-band Transmission Level
ATN Average Total Noise
BB Broadband
CENELEC Committee for Electrotechnical Standardization
CIFS Contention Interframe Space
CO Channel Occupancy
COALE Channel Occupancy Active link-estimation
CSMA/CA Carrier Sense Multiple Access with Collision Avoidance
CTP Collection Tree Protocol
D8PSK Differential Eight Phase Shift Keying
DAG Directed Acyclic Graph
DAO ACK DAO Acknowledgment
DAO Destination Advertisement Object
DBPSK Differential Binary Phase Shift Keying
DC Data Concentrator
DIO DAG Information Object
DIS DAG Information Solicitation
DIS-NA DIS No Answer
DODAG Destination Oriented DAG
DQPSK Differential Quaternary Phase Shift Keying
DSP Digital Signal Processor
DTSN DAO Trigger Sequence Number
E2E End-to-End
EIFS Extended Interframe Space
ETX Expected Transmission Count
EWMA Exponentially Weighted Moving Average
FCC Federal Communications Commission
FCH Frame Control Header
FRLD Fast and Reactive Link-failure Detection
FSM Finite State Machine

G3-PLC G3-PLC
HAN Home Area Network
HE2M Head-End-to-Meter
IEEE Institute of Electrical and Electronics Engineers
IETF Internet Engineering Task Force
IFS Inter Frame Spacing
IP Internet Protocol
IPv6 Internet Protocol version 6
LF NB Low Frequency Narrowband
LF Low Frequency
LLN Low power and Lossy Network
LOAD 6LoWPAN Ad Hoc On-Demand Distance Vector Routing
LOADng Lightweight On-demand Ad hoc Distance-vector Routing Protocol Next Generation
LQI Link Quality Indicator
LV Low Voltage
M2HE Meter-to-Head-End
MAC Medium Access
MANET Mobile Ad-hoc Networks
MDMS Meter Data Management Systems
MP2P Multipoint-to-Point
MRHOF Minimum Rank with Hysteresis Objective Function
MV Medium Voltage
NAN Neighborhood Area Network
NB Narrowband
NIST National Institute of Standards and Technology
NM Node Model
NS Neighbor Solicitation
NUD Neighbor Unreachability Detection
NUD-PP Neighbor Unreachability Detection for Preferred Parent
OCP Objective Code Point
OF Objective Function
OF0 Objective Function Zero
OFDM Orthogonal frequency-division multiplexing
ORPL Opportunistic RPL
OS Operating System
P2MP Point-to-Multipoint
P2P Point-to-Point
PCS Physical Carrier Sense
PDR Packet Delivery Ratio
PHY Physical
PLC Power Line Communication
PM Process Model

RERR Route Error
RFC Request For Comments
RIFS Response Interframe Space
ROBO Robust Orthogonal Frequency Division Multiplexing
ROLL Routing over Low-Power and Lossy Links
RPL RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks
RREP Route Reply
RREP-ACK Route Reply - Acknowledgment
RREQ Route Request
SG Smart Grid
SINR Signal-To-Noise Interference-Ratio
SM Smart Meter
SNR Signal Noise Ratio
TM Tone-Map
TMReq Tone-Map Request
TMResp Tone-Map Response
UNB Ultra Narrow Band
WAN Wide Area Network
WSN Wireless Sensor Network

Contents

1 Introduction

Strange about learning;
the farther I go
the more I see that I never knew even existed.
A short while ago I foolishly thought I could learn everything
- all the knowledge in the world.
Now I hope only to be able to know of its existence,
and to understand one grain of it.
Is there time?

Daniel Keyes, Flowers for Algernon

Ever since man has tamed electricity, the means for producing and distributing it have been in gradual evolution. The biggest change to the power grid in the past several decades is the recent effort to deploy Internet technologies throughout the grid in order to turn the grid into a *Smart Grid* (SG). Nowadays, more than ever, the grid has to meet new challenges and constraints:

- Efficient management of production and distribution of power;
- Provide feedbacks about real-time pricing information and consumption to users;
- Integration of renewable energy sources, electrical vehicles;
- Real-time demand response and management strategies for lowering peak demand and overall load, through appliance control;
- Integration of locally distributed micro-generation sources.

From the distribution part, former generation of power grid only allowed to collect limited informations (kWh reading and possibly peak kW demand for the month) in a one-way manner. The new power grid needs to have a real-time, accurate knowledge of the actual energy consumption all along the grid and to be able to communicate bidirectionally with all the elements connected to the grid – the essence of the SG.

We can see on Figure 1.1 that two domains can be distinguished on the current power grid: the *operated* (generation, transmission and distribution of electricity) and the *customers* domain. The frontier between the two is of crucial importance – classically for accounting purposes, and since recently – for enhanced grid operation

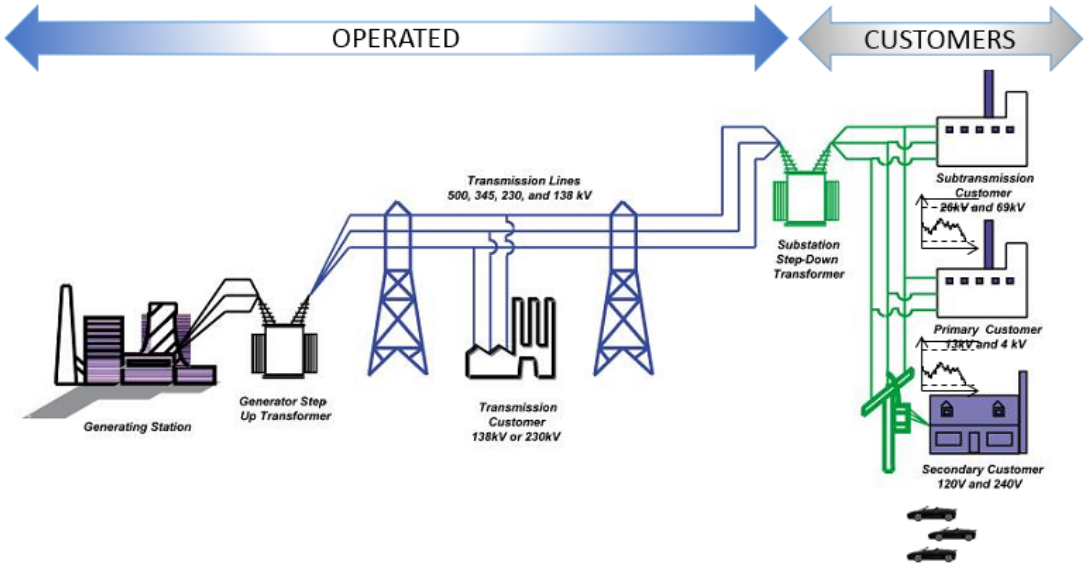


Figure 1.1: The power grid. (source: *www.nerc.com*)

and control, e.g. demand side management (stopping air conditioning for a couple of minutes during peak hours) or two-way energy flow control (e.g. when a customer has local energy production and injects it to the grid). This border is materialized in the majority of the cases by the power meter.

Having a two-way communication channel with a computerized power meter, i.e. *Smart Meter* (SM), is therefore one of the pillars of the Smart Grid. In some cases, the SM can be reached directly through an existing *Wide Area Network* (WAN) technology (such as a cellular network), but a multitude of factors often imposes the usage of a dedicated local network which connects the meters in proximity, such as a neighborhood or the ones connected to the same power transformer – a *Neighborhood Area Network* (NAN).

The system which englobes the SMs, the networks necessary to communicate with them (NAN and WAN), and the backend management system is called *Advanced Metering Infrastructure* (AMI). AMI relies on efficient and robust NAN to carry information between power meters and a *Data Concentrator* (DC). DCs are the elements which connect the NAN to the WAN, and can vary in complexity – from a simple repeater to a full-featured application-level gateway (Figure 1.2). In this thesis, we are going to focus on AMI environment and more specifically on communications between DC and SMs – the last-mile of an AMI. AMI is a key enabler of the Smart Grid as it permits to monitor in real-time the power consumption and allows utilities to act and react to system's evolution.

At the present time, there are close to 45 million Smart Meters already installed in three European Member States (Finland, Italy and Sweden). The European Commission stated that by 2020, 200 million SMs for electricity (representing ap-

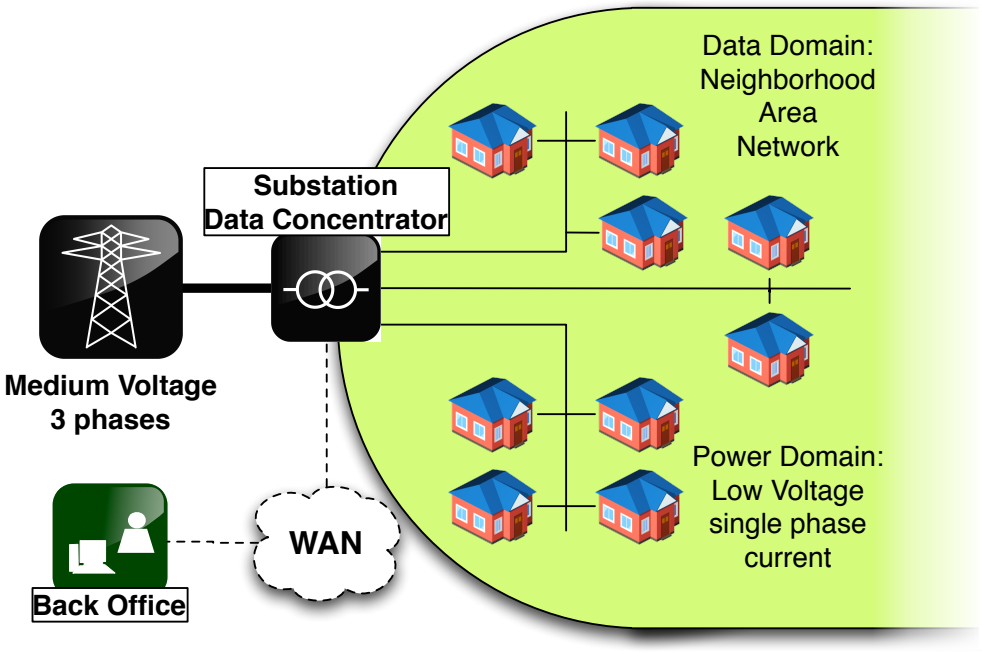


Figure 1.2: Elements of an Advanced Metering Infrastructure.

proximately 72% of all European consumers) should be deployed [EL14]. Despite recent efforts produced to define a Smart Grid framework [GOEED14] and the fact that SMs deployments already started worldwide, Smart Grid is today more a "vision" than an actual design and a wide variety of choices has yet to be made by utilities, such as selecting:

- Physical medium (wireless or wired) i.e. the medium used to propagate the data;
- Upper layer network stack in order to transmit and route traffic between SMs and utilities.

Concerning the physical medium, two choices can be made: wired or wireless medium. One of the most promising solutions to carry data in the power grid is a wired solution: *Power Line Communication* (PLC). PLC allows to transport data on the electric power line and offers a big advantage compared to wireless solutions: as power lines are already installed, PLC deployment cost is limited. Thus, PLC has been selected by utilities and power meter industry as a potential candidate for physical medium. However, due to its intrinsic harsh characteristics (noise, low throughput, etc.), usage of PLC in Smart Grid environment presents specific challenges that need to be addressed with adapted PLC solutions. To that purpose, a large part of PLC industry's technical experts and stake holders specified the P1901.2 [IEE10] which has been standardized by *Institute of Electrical and Electronics Engineers* (IEEE). It uses low frequency narrowband (<500kHz) that can provide throughput up to 500kbps depending on regulatory bands. In this

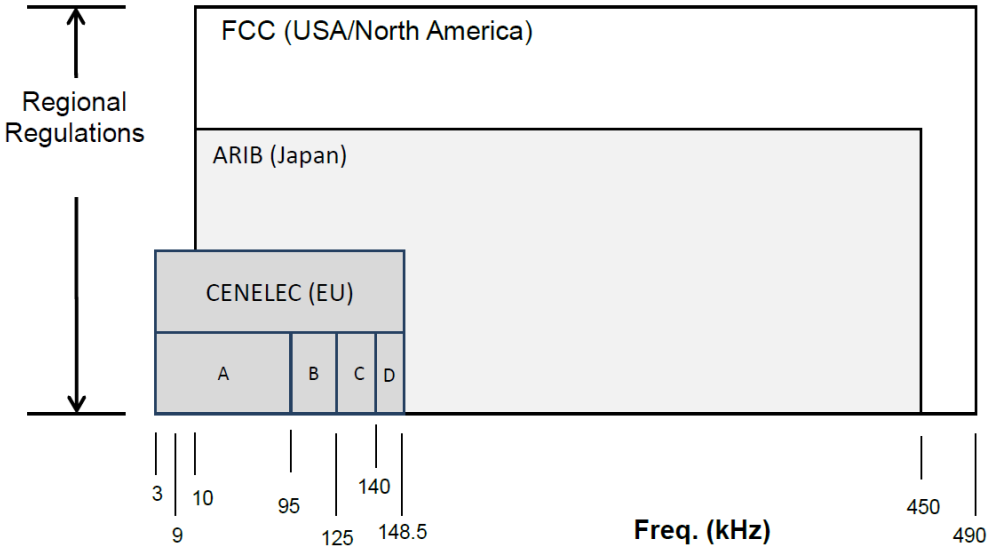


Figure 1.3: Regulatory frequency map. (source:[IEE10])

thesis, our work is based on IEEE P1901.2, and more precisely in *Committee for Electrotechnical Standardization* (CENELEC) A band: the band reserved for power companies in Europe (Figure 1.3).

The choice of physical medium is not the only one that needs to be made by utilities, upper layer network stacks is of crucial importance. IEEE P1901.2 imposes the use of *Internet Protocol version 6* (IPv6). The motivation to choose an IP solution is based on IP success as a convergence layer (more than two billions people use the Internet daily) and its past history (30 years of technology development) which facilitates open standards and interoperability. IPv6, with its new functionalities (auto-configuration, larger address space, etc.) is the ideal solution for new networks and has thus been selected by utilities for Smart Grid's deployment.

While IPv6 has been widely adopted as a key component of SG environment, debates are opened and ongoing for the routing protocol to use. PLC networks, with their characteristics, can be seen as *Low power and Lossy Network* (LLN) (i.e. a network of constrained devices). The *Internet Engineering Task Force* (IETF) working group *Routing over Low-Power and Lossy Links* (ROLL) designed a routing protocol specifically for LLN. This protocol, *RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks* (RPL) [WTB+12], allows to construct and install loop-free routes thank to a *Directed Acyclic Graph* (DAG) rooted at a single destination: the sink. It permits to have bidirectional routes from sensors to the sink (from SMs to the DC in AMI architecture) which fits with the SG primary goal: bidirectionality of the communications. RPL has been mainly designed for *Multipoint-to-Point* (MP2P) traffic (even if it allows *Point-to-Point* (P2P), as well as *Point-to-Multipoint* (P2MP) traffics), and more precisely aims to optimize routes from the sensors to the data sink.

At present, RPL performances have been widely studied in the literature in the context of *Wireless Sensor Network* (WSN), but few results are available about RPL in PLC environment and even less in PLC AMI architecture. AMI environment traffic patterns have been identified and categorized in two parts in [draa]:

- *Meter-to-Head-End* (M2HE);
- *Head-End-to-Meter* (HE2M).

HE2M traffic is of crucial importance as it allows utilities to communicate with SMs for event-based traffic (e.g. to stop some equipments, to trigger spontaneous meter readings, or to update firmware). RPL must thus be studied in AMI PLC environment to analyze its effectiveness for every AMI typical traffic pattern and to determine if optimizations specially tailored for AMI are needed.

1.1 Contributions

In order to study RPL protocol performances, we designed and implemented a complete IEEE P1901.2 simulator under OPNET. This phase includes the proposition and implementation of a IEEE P1901.2 PLC channel model as well as the complete development of a IEEE P1901.2 RPL simulator under OPNET . We also implemented *6LoWPAN Ad Hoc On-Demand Distance Vector Routing* (LOAD) [LOAa] and its evolution *Lightweight On-demand Ad hoc Distance-vector Routing Protocol Next Generation* (LOADng) [LOAb]. We decided to use LOAD and LOADng as baseline comparison. Indeed, LOAD and LOADng protocols have been chosen as the default routing protocols for G3-PLC [G3-], an other narrowband PLC standard defined for Smart Grid. To evaluate a PLC technology, the AMI industry relies on performance metrics reported on large scale cells (1500 nodes per data concentrator), on a wide range of topologies (rural, urban, mixed) and on different impedance and noise profiles. Real field evaluations are generally limited to a small numbers of nodes, topologies and noise profiles. The main limitation is the resources and logistic costs related to pilot deployments. The only alternative to real field deployments are simulation-based evaluations. Our simulation results have been validated against real testbed implementation [RLP+] in order to have the needed confidence for results analyses.

Our main contribution is to propose adaptations and optimizations to RPL protocol specially tailored for IEEE P1901.2 AMI environments. Enhancements can be categorized in two parts:

- Route Formation: The process to create bidirectional routes between SMs and DC at RPL startup [RLP+14];
- Route management: The phase when RPL reaches its steady-state and that routes need to be maintained and updated based on events (link-quality change, link-breakage, or non-working SM).

Our goal has been to minimize RPL overhead, convergence time, repair time in case of link-breakage and *End-to-End* (E2E) delay, while maximizing *Packet Delivery Ratio* (PDR). We propose a distributed approach solution *Distributed Dynamic DelayDAO interval adjustment* (4Dia) [RLP+14] in order to improve route formation convergence time. This method, computing dynamically signaling messages emission regarding to network conditions in order to avoid congestions, allows to speed-up the route formation process in AMI context. We also introduced a new definition for convergence time in AMI environment by highlighting the fact that bidirectional communication brings new requirements.

We enhance route management by adding a novel method to react to link-breakage or non-working SM: *Fast and Reactive Link-failure Detection* (FRLD). This mechanism is based on a slightly modified version of *Neighbor Unreachability Detection* (NUD). It allows to accelerate both link-breakage and non-working SM detection as well as the installation of new needed routes to react to that outage. We also reduce RPL signaling overhead by adding new criteria to manage DAO emission based on utilities feedbacks.

Finally, we introduce a new metric for RPL: the *Channel Occupancy* (CO) metric [RLP+15]. CO aims to minimize the global channel occupation by computing path costs based on the usable modulation for each link. Thus, routes are constructed by minimizing channel occupancy. In opposition to *Expected Transmission Count* (ETX) [DCABM03] metric, CO may use more hops to relay data but End-to-End delay is going to be lowered while PDR is maximized. We designed the metric usage for both RPL Objective Functions (OFs) defined so far: *Objective Function Zero* (OF0) and *Minimum Rank with Hysteresis Objective Function* (MRHOF). Our solution is implemented for IEEE P1901.2 environment but could be applied to other environments.

1.2 THESIS OUTLINE

Chapter 2 presents the context of this thesis and more particularly introduces the Smart Grid and one of its key component, the AMI, prior to present a classification of existing PLC solutions to locate IEEE P1901.2 in the PLC galaxy. The Chapter will be concluded by a description of IEEE P1901.2.

Chapter 3 describes in details RPL routing protocol: what lead to its design genesis, its companion draft as well as its main mechanism. We introduce also in this chapter two other candidate routing protocols for *Low power and Lossy Network* (LLN): *6LoWPAN Ad Hoc On-Demand Distance Vector Routing* (LOAD) and *Lightweight On-demand Ad hoc Distance-vector Routing Protocol Next Generation* (LOADng).

Chapter 4 introduces the simulator developed in this thesis by a short overview of its implementation, its mains characteristics and the physical model used for

representing PLC channel, as well as a validation against a real-testbed.

Chapter 5 focuses on a weakness of RPL protocol for Smart Grid we detect when we analyze route formation's phase and the proposed mechanism to overcome that weakness: 4Dia .

Chapter 6 describes *Fast and Reactive Link-failure Detection* (FRLD) solution that enables fast and reactive link-failure detection specially tailored for taking into account SG traffic pattern characteristics.

Chapter 7 highlights the main drawbacks of *Expected Transmission Count* (ETX) metric in SG environment and introduces a new metric for RPL: *Channel Occupancy* (CO).

Chapter 8 presents the general conclusions of this work and the possible future research directions.

1

2 IEEE P1901.2: A narrowband PLC protocol for the Smart Grid

IEEE P1901.2 is a standard defined for low frequency (less than 500 kHz) narrowband communications PLC devices via alternating current and direct current electric power lines. This standard supports indoor and outdoor communications over *Low Voltage* (LV) (less than 1000 V) and *Medium Voltage* (MV) (1000 V to 72 kV) power lines and through associated transformers in both urban and long-distance rural applications. Data rates will vary up to 500 kbps depending on the application requirements and network conditions. This standard addresses grid to utility meter, grid automation, electric vehicle to charging station, and within home area networking communications scenarios.

In this chapter, prior to describe IEEE P1901.2, we introduce the *Smart Grid* (SG) in Section 2.1 in order to understand its role and the new challenges associated to it. Then, in Section 2.2, we describe a key component of the SG: the *Advanced Metering Infrastructure* (AMI). A classification of PLC is then presented for understanding the position of IEEE P1901.2 in respect to the existing standards. Finally, IEEE P1901.2 is described in Section 2.3.

2.1 The Smart Grid

Domain	Role
Customer	End-user of electricity (households, companies)
Operators	Operators and participant in electricity markets
Service provider	Organizations providing services to electrical customers and to utilities
Operations	Manager of movement of electricity
Generation	Generators of electricity
Transmission	Carriers of bulk electricity over long distances
Distribution	Distributors of electricity to and from customers

Table 2.1: NIST conceptual domains for the Smart Grid.

The *Institute of Electrical and Electronics Engineers* (IEEE) defines the Smart Grid as *"a next-generation electrical power system that is typified by the increased*

use of communications and information technology in the generation, delivery and consumption of electrical energy". However, Smart Grid is such a complex system which involves several technical domains (IT, Telecom, Embedded Platforms, Advanced Control, Cyber Security, Power Electronics and Energy Engineers and Specialists) that its definition may vary depending on each domain perspectives. The *National Institute of Standards and Technology* (NIST) defined a Framework and Roadmap for Smart Grid. It analyses existing standards, as well as major organisations involved, and provides recommendations for addressing the Smart Grid challenges [NIS]. The NIST introduces in [NIS] a conceptual model for the power grid (Figure 2.1) which identifies several domains (Table 2.1) and their interactions to enable the implementation of the Smart Grid.

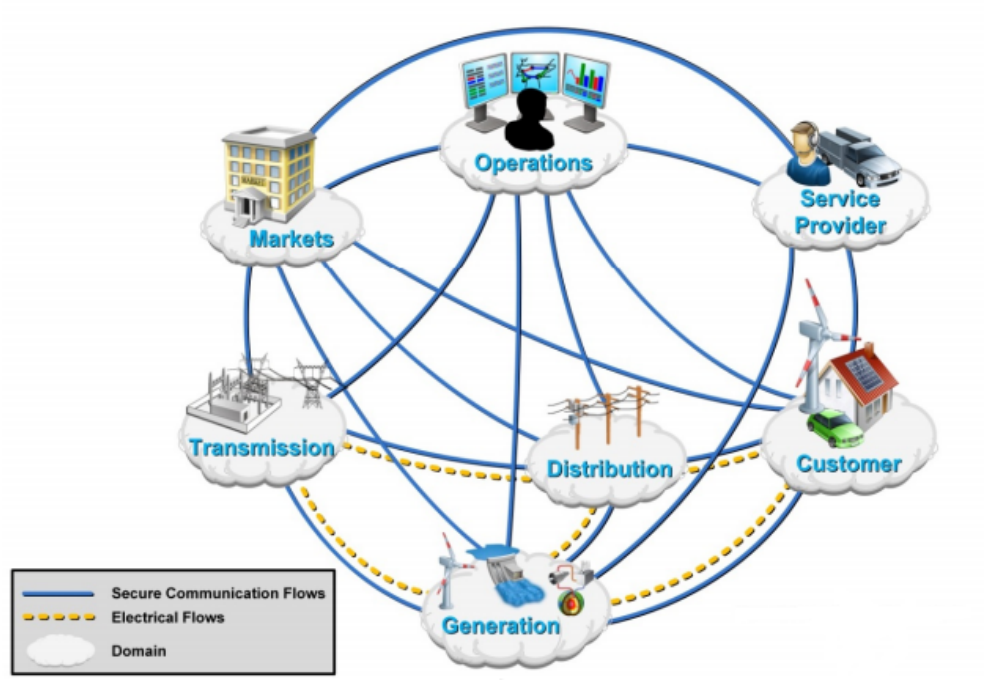


Figure 2.1: Conceptual domains interactions Grid. (source: www.nist.com)

These different domains interact in order to create additional functionalities compared to the former power grid:

- Enables real-time analysis of power system components performances across large areas in order to improve efficiency and react before perturbations occur;
- Provides an opportunity for consumers to adapt their electrical consumption by reducing or shifting their electricity usage during peak periods depending on real-time pricing (Demand Response);
- Integrates generation (renewable energy) and/or electric storage systems;
- Manages the emergence of electrical vehicle.

From communications perspective, Smart Grid appears as the interconnection of several networks (Figure 2.2): the *Home Area Network* (HAN), the *Neighborhood*

Area Network (NAN) and the *Wide Area Network* (WAN). The HAN is the network that allows communications between smart devices and appliances within the household (or buildings). For examples, it could be the display of real-time energy consumption on a smartphone, as well as automatically turning-off a thermostat based on utilities pricing. The NAN is the local network that permits the communication between each device in a limited area (e.g. neighborhood). In the Smart Grid context, Smart Meters are connected with a *Data Concentrator* (DC) over a NAN. The WAN allows device in a large area to communicate. From Smart Grid perspective, this network makes the interconnection between utilities and the data collected by the Smart Meters (SMs) in the NAN, the DC being in charge of NAN and WAN interconnexion.

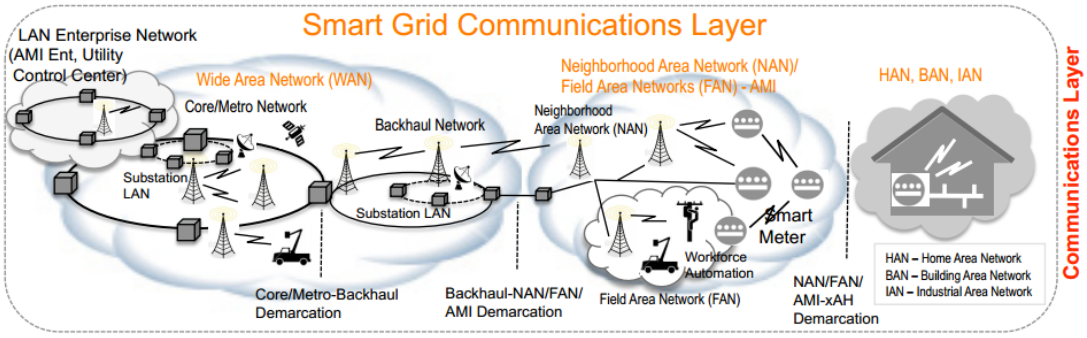


Figure 2.2: Smart Grid from communications Point of View. (source: *IEEE*)

2.2 The AMI

The *Advanced Metering Infrastructure* (AMI) is the part of the Smart Grid that allows to connect SMs to the utilities *Meter Data Management Systems* (MDMS) in order to manage collected data. From communication networks perspective, AMI is using NAN and WAN. The main architecture used for AMI is made of one DC that acts as a gateway between the WAN (to the utilities) and the NAN (the gathered information from the SMs). In this thesis, we focus on the NAN communication network between SMs and DC.

2.2.1 AMI technologies

Various technologies (wired or wireless) can be used to connect SMs and DC [GSW10]:

- wired: *PON* (*GPON*, *EPON*), *RFoG-DOCSIS*, *PLC*;
- wireless: *RF Mesh/802.15.4g*, *Wimax 802.16d/e*, *RF Radio Pto-Mtp/MAS*, *3G-3GPP/1XRTT/EVDO*, *GPRS/EDGE/HSDPA*, *WLAN 802.11 n/g*, *802.2.15.4/ZigBee*.

Compared to wireless solutions, PLC offers several advantages. Indeed, the power-line infrastructure is already existing and reusing it allows to lower the deployment costs. Additionally, SMs location is not always compatible with the use of wireless technologies (for example, it is not rare in Europe to find meters inside household surrounded with concrete walls or steel). The power-line network is also managed and owned by utilities which allow them to have full control on the network contrary to wireless technologies (which also have the drawback to use a public Radio Frequency band). For all these reasons, PLC has been selected by utilities as a candidate technology to be used in AMI environment.

PLC does not refer to only one protocol or technology. In the next section, we are going to describe the existing solutions for PLC and their main characteristics.

2.2.2 PLC classification

PLC can be classified in three categories [GSW10] depending on the frequency range:

1. *Ultra Narrow Band* (UNB) PLC: Ultra Low Frequency (0.3-3kHz) band or in the upper part of the Super Low Frequency (30-300 Hz) band;
2. *Narrowband* (NB) PLC: Very Low Frequency/Low Frequency /Medium Frequency bands: (3–500kHz);
3. *Broadband* (BB) PLC: lower frequencies (1.8–250MHz): High Frequency/Very High Frequency bands (1.8-250 MHz).

UNB band operates in the 0.3–3kHz band. While throughput can be considered as low (around 100bps), long distances can be crossed (over 150 km) with UNB PLC. Examples of UNB PLC utilizations are *ripple carrier signaling*, *turtle system* and more recently *Two-Way Automatic Communication System (TWACS)*. It has to be noted that at the present time, no standard is existing for UNB PLC and that the aforementioned examples are proprietary solutions.

NB PLC operates in the frequency range from 3 kHz to 500 kHz (Figure 1.3), including the European *Committee for Electrotechnical Standardization* (CENELEC) bands (3–148.5 kHz), the US *Federal Communications Commission* (FCC) band (10–490 kHz), the Japanese *Association of Radio Industries and Businesses* (ARIB) band (10–450 kHz) and the Chinese band (3–500 kHz). NB PLC offers range up to several kilometers and data rate up to 500kbps. [GSW10] proposed a classification for NB PLC:

- Low data rate (LDR): provides throughput of few kbps based on single carrier technology. A wide variety of standards exists such as *ISO/IEC 14908-3 (LonWorks), ISO/IEC 14543-3-5 (KNX), CEA-600.31 (CEBus), IEC 61334-3-1, IEC 61334-5 (FSK and Spread-FSK)*;
- High data rate (HDR) multicarrier communication, such as Orthogonal Fre-

Categories	Frequency Range	Data Rates	Technologies
UNB PLC	0.3–3kHzHz	100bps	ripple TWACS turtle
NB PLC	3–500kHz	few kbps	ISO/IEC 14908-3 ISO/IEC 14543-3-5 CEA-600.31 IEC 61334-3-1 IEC 61334-5
		up to 500kbps	PRIME G3-PLC ITU-T G.hnem **IEEE P1901.2**
BB PLC	1.8–250MHz	200Mbps	TIA-1113 (HomePlug 1.0) IEEE 1901 ITU-T G.hn (G.9960/G.9961)

Table 2.2: PLC classification.

quency Division Multiplexing (OFDM), capable of data rates ranging between tens of kbps and up to 500 kbps. Typical examples of HDR NB PLC technologies are *G3-PLC, ITU-T G.hnem, and IEEE P1901.2.*

BB PLC (operating in the 1.8–250MHz) frequency range allows high data rates (up to 200Mbps). *TIA-1113 (HomePlug 1.0), IEEE 1901, and ITU-T G.hn (G.9960/G.9961)* are examples of BB PLC technologies.

Table 2.2 summarizes characteristics of UNB, NB, and BB PLC technologies.

2.2.3 AMI traffic pattern

In order to choose an adequate PLC solution for AMI, traffic patterns needs to be characterized. [draa] defines traffic pattern requirements in AMI environment in two classes:

- From the utility Head-End server to SMs: *Head-End-to-Meter* (HE2M) traffic;
- From SMs to the Head-End server: *Meter-to-Head-End* (M2HE) traffic.

The notion of Head-End server refers to any server operated by the utilities and that is located in the WAN. Head-end server sends traffic for:

- SM configuration: a configuration change (e.g., change the schedule of SMs periodic energy consumption report) as well as firmware update;
- SM queries: request a meter read request.

SMs generate scheduled traffic (e.g., periodic meter reads), event-based traffic (e.g. power outage) or based on on-demand requests (e.g., meter read requested by Head-end server).

Figure 2.3 depicts M2HE and HE2M traffic in AMI infrastructure.

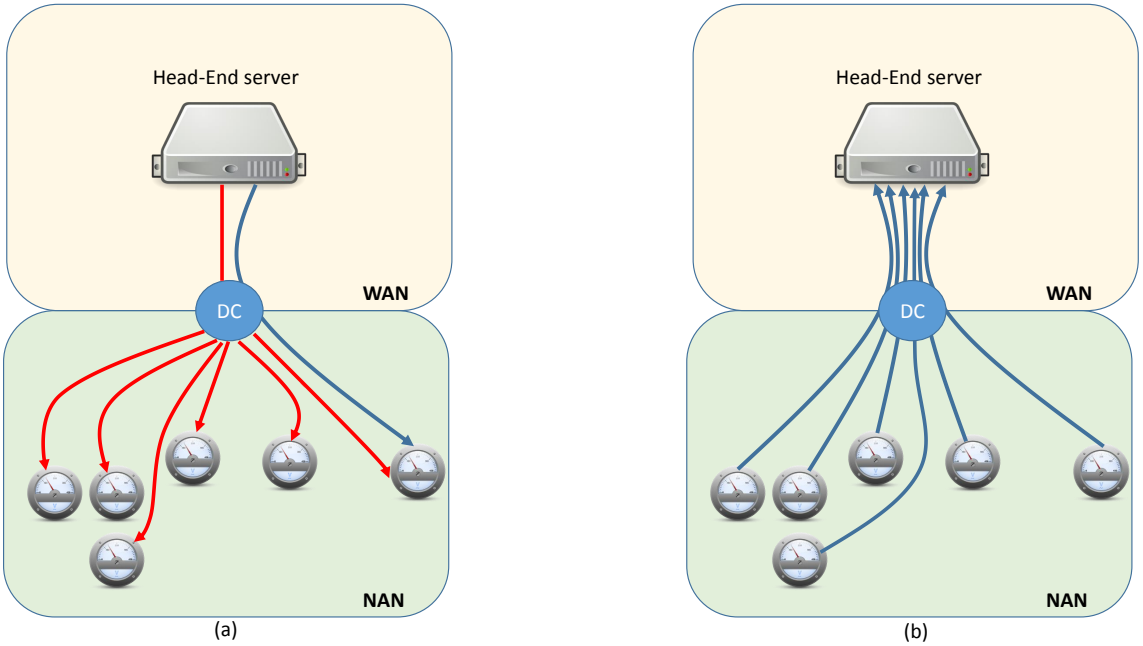


Figure 2.3: Traffic Pattern inside AMI. (a) stands for HE2M traffic and (b) for M2HE traffic pattern. Blue arrow represents unicast traffic while red one represents multicast traffic.

Head-end server can either reach a specific SM directly in a unicast way (*Point-to-Point* (P2P)) or can reach a group of devices by using multicast (*Point-to-Multipoint* (P2MP) while SMs usually send traffic to a specific head-end server in an unicast way and generate *Multipoint-to-Point* (MP2P) traffic.

2.3 IEEE P1901.2

In 2009, *Institute of Electrical and Electronics Engineers* (IEEE) decided to create the working group P1901.2 to standardize a *Low Frequency Narrowband* (LF NB) (<500 kHz) PLC solution. Indeed, at that time, no standard was existing for such kind of technology as shown on Table 2.3.

The IEEE P1901.2 [IEE10] standard is designed for indoor and outdoor electrical wiring *Power Line Communication* (PLC) over low voltage (<1000V) and medium voltage (1000V to 72kV). The standard employs techniques and mechanisms defined in two related standards covering the same scope, namely: *G3-PLC CENELEC A* (*ITU-T G.9903*) and *PRIME CENELEC A* (*ITU-T 3 G.9904*). IEEE

Standards and proprietary solutions	Frequency Band	Data Rate
IEC 61334	CENELEC	2.4kbps
ISO/IEC 14908-1	CENELEC	5.0kbps
HomePlug CC	CENELEC	7.5kbps
LF NB Maxim Integrated MAX2990	CENELEC - FCC	100kbps
LF NB G3-PLC	CENELEC -FCC	100kbps
LF NB PRIME	CENELEC	125kbps
HomePlug 1.0	>2MHz	14Mbps
IEEE P1901 Dual PHY/MAC	> 2MHz	200Mbps
ITU G.hn	> 2MHz	200Mbps

Table 2.3: Existing PLC standards and proprietary solutions in 2009 for Low and High Data Rate PLC.

P1901.2 can operate in three different bands to overcome global regulations problem: the *Committee for Electrotechnical Standardization* (CENELEC) band in Europe (CENELEC bands A, B, C, and D), which has an upper limit of approximately 150kHz; the *Association of Radio Industries and Businesses* (ARIB) band (Japan), which has an upper limit of approximately 450kHz; and the *Federal Communications Commission* (FCC) band (multiple countries), which has an upper limit of approximately 500kHz. In this thesis, we focus on IEEE P1901.2 standard in the CENELEC A band as it is the spectrum reserved for power companies in Europe.

The physical characteristics of *Narrowband* (NB) PLC resembles the ones of low-power, lossy radio links. As a consequence, IEEE P1901.2 reuses parts of the *Medium Access* (MAC) layer and channel access methods of IEEE 802.15.4 [GCB03]. However, as IEEE P1901.2 uses several modulations, a *Physical* (PHY) layer header was added to specify parameters relative to the payload.

2.3.1 Physical layer

IEEE P1901.2 uses *Orthogonal frequency-division multiplexing* (OFDM) and supports two different modulation schemes:

- Differential mode (mandatory) modulations: *Differential Binary Phase Shift Keying* (DBPSK), *Differential Quaternary Phase Shift Keying* (DQPSK), and *Differential Eight Phase Shift Keying* (D8PSK);
- Coherent mode (optional) modulations: BPSK, QPSK, 8PSK, and 16QAM.

It has to be noted that both modes share a default robust modulation: *Robust Orthogonal Frequency Division Multiplexing* (ROBO).

We decided to focus on the mandatory mode in that thesis. IEEE P1901.2 CENELEC A band works specifically in the 35kHz–91kHz band range [IEE10] and

uses OFDM modulation over 36 carriers.

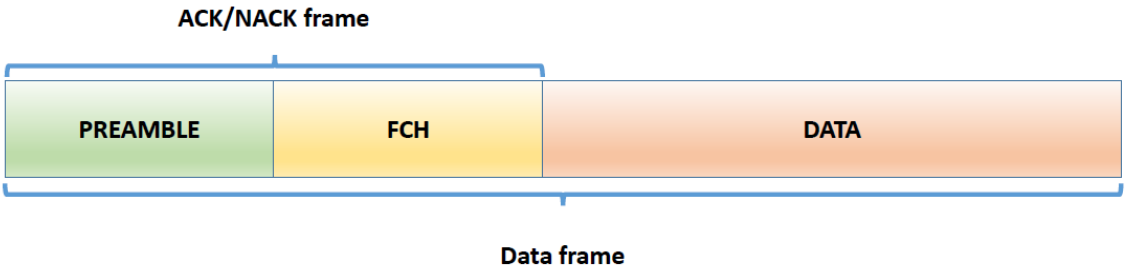


Figure 2.4: IEEE P1901.2 frame structure.

The PHY layer supports two type of frames: data and ACK/NACK. Frame structure is shown in Figure 2.4. Each frame starts with a preamble, followed by the *Frame Control Header* (FCH). ACK/NACK frames are only made of Preamble+FCH while data frames are followed by the data itself.

The preamble is used for synchronization, channel estimation and initial phase reference estimation. The FCH includes information such as the type of frame, its length, modulation and Tone-Map mechanism described in Section 2.3.3.

2.3.2 MAC layer

The MAC layer frame follows the FCH and is based on the IEEE 802.15.4 with almost identical structure. It has to be noted that IEEE P1901.2 does not use classical IEEE 802.15.4 MAC acknowledgment frames to confirm unicast frames. Instead, it specifies positive and negative acknowledgments in the FCH as explained above. Thus, IEEE P1901.2 acknowledgments can be seen as PHY ACK.

2.3.2.1 Channel access

Channel access is performed thanks to *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA) with a random backoff time. The random backoff mechanism is used to spread the time over which stations attempt to transmit in order to reduce the probability of collisions. Each time a device wishes to transmit data frames, it waits for a random period. If the channel is idle after that period, the device is able to transmit its data frame. If the channel is busy after the random backoff time, the device has to wait an other random period before to access the channel again. In order to detect channel occupancy, *Physical Carrier Sense* (PCS) is used.

IEEE P1901.2 defined two CSMA/CA modes: an unslotted version for the mandatory non-beacon PAN described in IEEE 802.15.4-2006 and a slotted version for the optional beacon-enabled PAN.

We decided to investigate the mandatory mode i.e the unslotted CSMA/CA mode. This mode ressembles to the IEEE 802.15.4 CSMA/CA but it is modified in order to take into acccount priority and fairness in order to improve efficiency. The algorithm implementation used unit of time called *backoff periods*. Each device maintains four variables for each transmission attempt:

- *NB*: the number of times the CSMA/CA algorithm was required to backoff while attempting the current transmission.
- *NBF*: count of backoff attempts and it is used to control channel access fairness.
- *minCWCount*: the number of time minimum contention window value was used to set backoff time.
- *CW*: contention window for each device. On device startup, the *CW* is initialized to *2macMinBE*. The device updates the *CW* based on channel access success or failure:
  - For every channel access failure, the CW value doubles. The maximum value of CW is bounded by *2macMaxBE*
  - Upon a successful transmission, the CW value is adjusted using the formula $CW[next] = max(CW[prev] - A * (2macMinBE, 2macMinBE)$

Figure 2.5 depicts in detail the steps of CSMA/CA algorithm. The main differences compared to IEEE 802.15.4 CSMA/CA mechanism occur in *Step 3* and *Step 7* that allow better fairness between devices; *Step 3* ensures fairness by comparing the number of time minimum contention windows (*minCW*) was used with the constant *maxMinCWAttempts*. If *minCW* is greater than *maxMinCWAttempts*, the *CW* is set to the maximum value *2macMaxBE*. Thus, it avoids the same device to always use the minimum contention window and then, helps other station to have access to the medium; *Step 7* is triggered when the channel was not found idle after the backoff timer. At that time, if the number of backoff attemps *NBF* is greater than the constant; *macCSMAFairnessLimit* and if *NBF* is multiple of K (Fairness Rate Adaptation Factor), the device is going to act as if the transmission was successful i.e. the CW is linearly decreased to allow for higher chance for pending frame transmission to succeed for devices which did not get the opportunity to transmit.

2.3.2.2 *Inter Frame Spacing* (IFS)

Due to propagation and processing time, a time interval is needed between frames: the *Inter Frame Spacing* (IFS). Figure 2.6 shows the different existing IFS:

- *Contention Interframe Space* (CIFS): used after the end of the previous transmission.
- *Response Interframe Space* (RIFS): the time between the end of a transmission and the start of its associated response. If no response is expected, the CIFS is in effect.

- *Extended Interframe Space* (EIFS): used when the station does not have complete knowledge of the state of the medium. This can occur when the station initially attaches to the network, when errors in the received frames make them impossible to decode unambiguously, or in the case a transmitter does not receive an ACK frame after a transmission for which the receiver was expected to issue an ACK to that transmitter. If a packet is received and correctly decoded before the expiration of the EIFS, then the EIFS is canceled.

2.3.3 Tone-Map mechanism

IEEE P1901.2 can use up to 4 modulations in mandatory mode: ROBO, DBPSK, DQPSK, and D8PSK. Additionally, IEEE P1901.2 works with 36 carriers (grouped in 6 sub-bands of 6 tones) in CENELEC A band, each sub-bands being usable depending on channel conditions. Thus, it renders the problem of selecting a path between two nodes non-trivial, as the possible number of combinations increases significantly, e.g. use a direct link with slow robust modulation, or use a relay meter with fast modulation and 2 disabled sub-bands. To overcome that problem, IEEE P1901.2 technology offers a mechanism for periodic exchanges on the link quality between nodes to constantly react to channel fluctuations – the adaptive *Tone-Map* (TM) mechanism. Every meter keeps a state of the quality of the link to each of its neighbors with whom it is communicating thanks to TM mechanism. When a device does not know the modulation to use for a particular neighbor, it must send the frame using ROBO mode and setting the *Tone-Map Request* (TMReq) bit in the FCH. Upon receiving a frame with the TMReq bit set, the receiver is going to estimate thanks to PHY preamble the communication link between the sender and the receiver and to choose the PHY parameters to use on this link. After the estimation, the receiver is going to generate a *Tone-Map Response* (TMResp) message. This frame contains the modulation to use, as well as the group of tones (i.e. sub-band) to use from frame transmission. It has to be noted that ROBO modulation must transmit using all the sub-bands.

2.4 Conclusion

In this chapter, we presented the big picture of the architecture used in this thesis: the *Smart Grid* (SG) and the *Advanced Metering Infrastructure* (AMI). We also made an overview of the existing PLC techniques and we presented one NB PLC technology that fits for AMI: IEEE P1901.2. Next Chapter will introduce RPL routing protocol main characteristics, as well as two other candidate routing protocols: LOAD and LOADng.

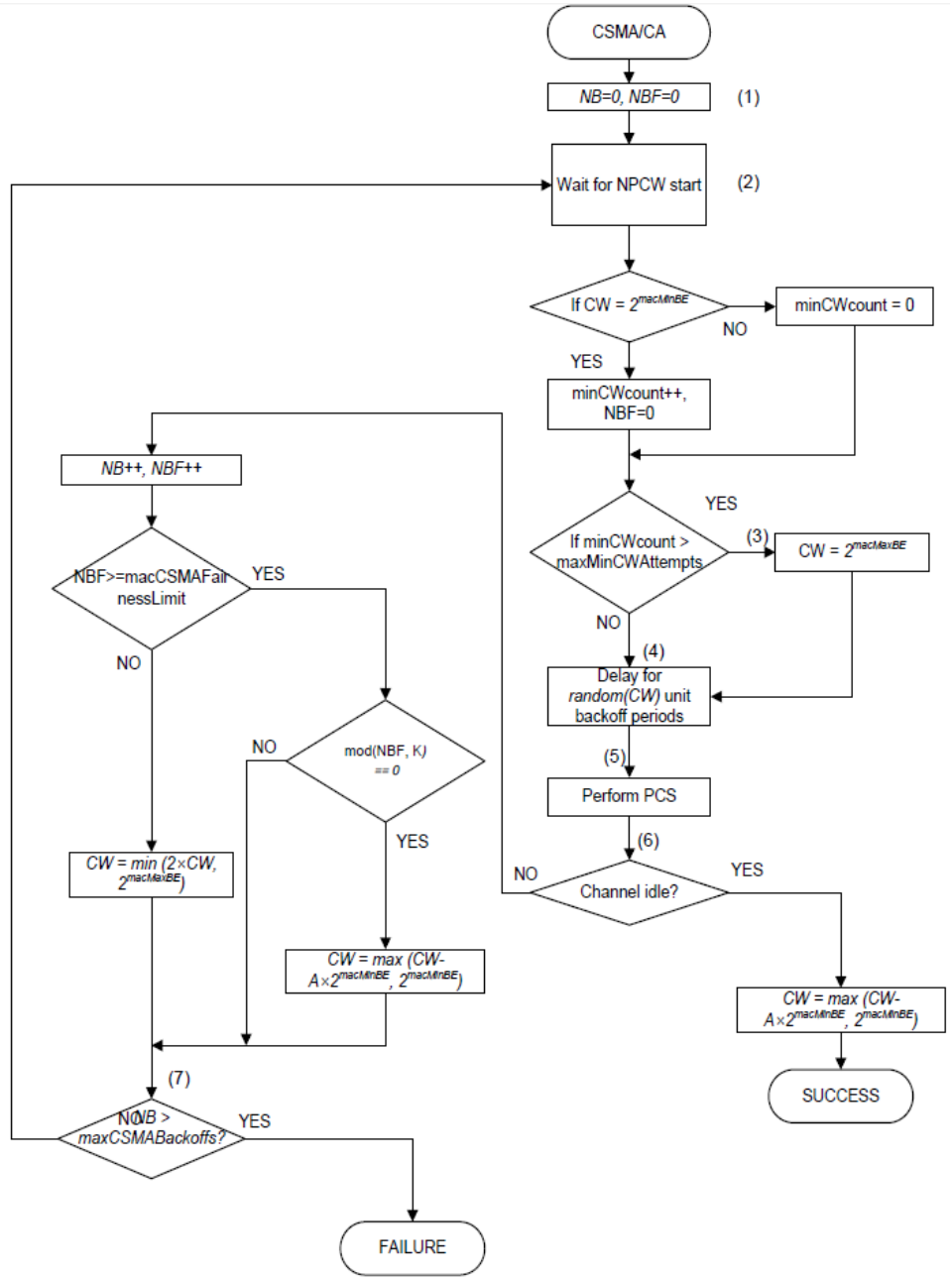


Figure 2.5: CSMA/CA unslotted mechanism. (*source: [IEE10]*)

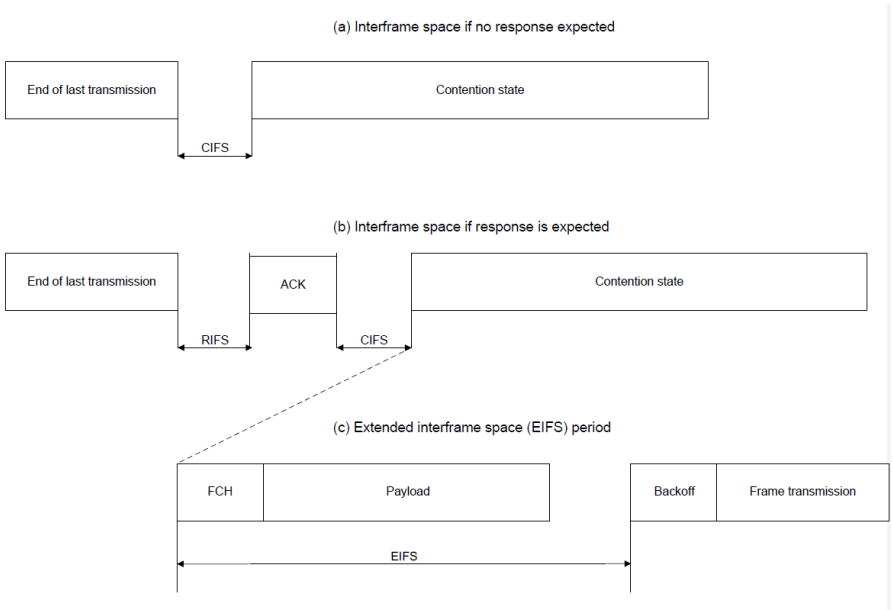


Figure 2.6: Inter Frame Spacing for IEEE P1901.2. (*source: [IEE10]*)

3 Routing Protocols

In the previous chapter, we highlighted that PLC characteristics lead to the development of new standardized solutions. In this chapter, we introduce a classification of routing protocols and more particularly, what lead to the design of new solutions specially tailored to Low power and Lossy Networks (LLNs). We present three routing protocols for LLN: *RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks* (RPL), *6LoWPAN Ad Hoc On-Demand Distance Vector Routing* (LOAD) and *Lightweight On-demand Ad hoc Distance-vector Routing Protocol Next Generation* (LOADng).

Section 3.1 presents the usual classification used for routing protocols (i.e. proactive or reactive) before to detail the need for new routing protocols specially designed for *Low power and Lossy Network* (LLN). Section 3.2 introduces two reactive routing protocols: LOAD and LOADng while Section 3.3 presents in detail the proactive protocol used in that thesis: RPL routing protocol.

3.1 Routing protocols

In a *Narrowband* (NB) *Power Line Communication* (PLC) IEEE P1901.2 infrastructure, it is impossible for most of the nodes to communicate directly due to various reasons: distance, noises, etc. Thus, each node must collaborate by relaying frames in order to be able to reach all nodes in the network. Routing protocols are designed to select, construct and maintain best paths in the network in order to route packets from source to destination. Traditionally, routing protocols are divided into two categories based on the way routing information is propagated namely: *proactive* and *reactive* protocols.

3.1.1 Reactive Protocols

Reactive protocols work by building routes on demand way and maintaining them only if needed. The main advantage compared to the proactive approach is that there is no need to maintain a route when there is no traffic and thus to be less greedy in term of resources. However, as the route does not exist before to its use,

a latency corresponding to the construction of the route is added.

One of the most well-known reactive protocol is the *Ad Hoc On-Demand Distance Vector Protocol* (AODV) [PBRD03]. AODV works by flooding the network with *Route Request* (RREQ) messages when it needs to send a data to a destination whose route is unknown. The Route Request is broadcasted until it reaches the destination or a node that has route information about the destination. Each node receiving and forwarding a Route Request keeps in its table an entry to the source of the flooding in order to be able to construct the reverse path for the *Route Reply* (RREP) message. Route Reply Messages are sent by an intermediate node or by the destination.

3.1.2 Proactive Protocols

Proactive routing protocols work on the principle that every node in the network must know a route to any destination at any time. Thus, a proactive protocol computes routes before they are needed. In this way, a node can transmit data to a destination without any additional delay just by looking in its routing table the corresponding entry. To maintain this routing table with up-to-date information, these protocols need periodic updates (i.e to send periodic messages). Transmission frequency must be sufficiently high to take into account the network's topology modification but not too high in order to avoid to overload the network with these signaling messages.

3.1.3 From MANET to ROLL

With the apparition of mobile wireless devices, new routing protocols specially tailored for mobility constraints started to appear. At a standardization level, the *Internet Engineering Task Force* (IETF) created the working group *Mobile Ad-hoc Networks* (MANET) in 1998 in order to design specific routing protocols that can deal with mobility. The developed protocols use two different techniques:

- *Flooding-based*: uses broadcast in order to transmit data and control packet in the network. Some examples of flooding-based protocols are *Dynamic Source Routing (DSR)*, *Ad Hoc On-Demand Distance Vector Protocol* (AODV) or *Dynamic Mobile On-Demand routing (DYMO)*;
- *Cluster-based*: the network is organized in clusters (a set of nodes) with one head cluster elected for each cluster. Data that must reach the sink is sent first to the cluster head before being transmitted to the sink. Cluster-based protocols can be used in conjunction with flooding-based protocol in order to reduce the flooding area. Some examples of cluster based protocols are *Low-Energy Adaptative Clustering Hierarchy (LEACH)*, the *Hybrid Energy-efficient Distributed clustering ptotocol (HEED)* or *Threshold sensitive Energy*

Efficient sensor Network protocol (APTEEN).

These routing protocols were developed with highly mobile nodes exchanging huge amount of data without energy constraints in mind (cars, smart-phone, etc.) [WMRD11]. However, the market tended to use cheaper and thus highly constrained devices for commercial application (such as monitoring, Smart Grid, etc.). The initial vision of MANET became obsolete for such kind of networks and even if some adaptations have been proposed to MANET protocols in order to work with constrained devices, in 2008, the *Routing over Low-Power and Lossy Links* (ROLL) working group has been created in order to standardize a specific routing protocol for *Low power and Lossy Network* (LLN). LLN has three main characteristics:

- They are composed of constrained devices (low processing power, memory, memory, and energy);
- The medium used to communicate exhibits fluctuating connectivity and losses, low throughput and instability;
- Main traffic pattern is *Multipoint-to-Point* (MP2P) flows.

3.1.4 LLN specific routing requirements

A wide variety of routing protocols were already existing before the apparition of LLNs but Levis *et al.* [drab] showed that none of them was meeting their requirements [drad] i.e:

- Multipath routing: help to ensure reliability by allowing the forwarding mechanism to select among multiple candidates;
- Resource awareness: As devices are constrained in LLN, the routing protocol must be able to take into account characteristics such as remaining energy, memory available, and not only the constraints imposed by the link quality;
- Small footprint: LLN devices often implement routing elements such as routing and neighbor tables on micro-controller device which has very poor capacities (few kilobytes of RAM and a few to several tens of kilobytes of program ROM);
- Small MTU: Prior to LLN, most of existing protocols were not implemented with limiting the MTU as a main purpose whereas this aspect is very important for LLN as MTU can be limited by the MAC Layer itself, as well as the fact that LLN transmission are subject to higher Bit Error Rates thus the shorter the transmitted frame is, the higher is the chance to receive it;
- Flooding Control and Density Awareness: Flooding is often used to discover routes. However, in LLN, flooding retransmission must be controlled in order to avoid broadcast storm and network collapse;
- Low power: Existing routing protocol tends to assume that devices are working in a "always on" mode while in LLN, devices will employ deep power managed techniques that could result in having the radio turned off for most of the time.

3.1.5 The need for new routing protocols for LLNs

Due to LLN characteristics, new LLNs-oriented routing protocols were defined including:

1. for reactive protocols
   - *6LoWPAN Ad Hoc On-Demand Distance Vector Routing* (LOAD) [LOAa] which is a simplified adaptation of AODV. This protocol provides optimizations to AODV to ensure better conformance with LLNs needs. In order to shrink the size of control messages and to simplify the route discovery process, LOAD does not use the destination sequence number. In LOAD, only the destination of a route generates a RREP in reply i.e the intermediate nodes should not respond with a RREP. This allows to guarantee a loop free topology. LOAD was chosen as the routing protocol for *ITU-T G.9903* first edition;
   - An improvement to LOAD, The *Lightweight On-demand Ad hoc Distance-vector Routing Protocol Next Generation* (LOADng) [LOAb] has been proposed. It provides enhancements to LOAD by supporting optimized flooding, and allowing the usage of custom metrics. LOADng has been chosen as the routing protocol for *ITU-T G.9903* third edition. LOAD and LOADng are described in Section 3.2.
2. for proactive protocols
   - IETF ROLL working group defined *RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks* (RPL) [WTB+12], a link-layer agnostic IPv6 routing protocol for LLN. RPL is based on a gradient-based approach [WMRD11] which is very efficient for sending all traffic to a single sink. A various number of protocols were already using gradient-based approach before RPL. In Gradient-Based-Routing [SS01], the gradient of the network is built based on the height of a node computed depending on the hop-count. The *Collection Tree Protocol* (CTP) [GFJ+09] uses the Expected Transmission Count (ETX) in order to compute the gradient. IETF ROLL decided to use that approach in order to satisfy the specific requirements of LLN.

LOAD and LOADng, being used as baseline comparison protocols, are going to be introduced in the next section.

3.2 LOAD AND LOADNG

6LoWPAN Ad Hoc On-Demand Distance Vector Routing (LOAD) [LOAa] and its evolution *Lightweight On-demand Ad hoc Distance-vector Routing Protocol Next Generation* (LOADng) [LOAb] are two reactive protocols designed for LLNs. LOADng is a new version of LOAD where many features have been reviewed to make the pro-

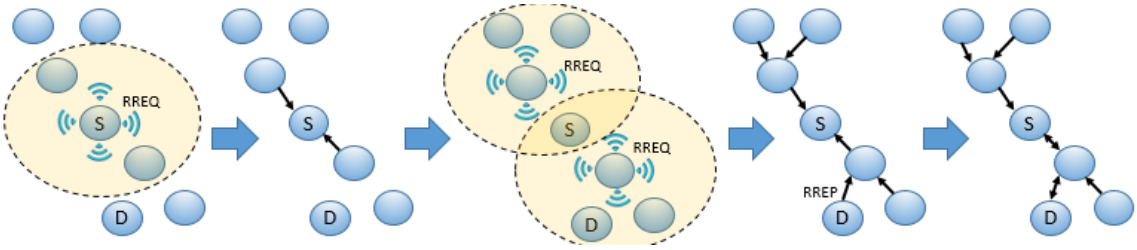


Figure 3.1: Route Construction for LOAD and LOADng. Light Yellow Circle represents RREQ transmission coverage.

tocol more extensible and more efficient.

The two protocols LOAD and LOADng share many common points:

1. When a router wants to transmit some data to a certain destination but does not have any information related to it in the routing table, it generates a *Route Request* (RREQ) message with the sought node as a destination address. The intermediate nodes broadcast the message. If one node receives a RREQ that it has already transmitted, it discards it to avoid breaking down the network. The intermediate nodes, upon receiving the RREQ, construct the reverse route to the originator;
2. When the RREQ reaches the final destination, this one can either generate immediately a *Route Reply* (RREP) message and then reduces the path establishment delay or waits until it receives a set of RREQs to choose the best path, that is, the path with the minimal metric. It is even possible for the router to generate further RREPs in case it receives RREQs with better metric at the expense of additional signaling traffic;
3. While forwarding the RREP to the originator of the corresponding RREQ, the intermediate nodes construct the forward route to the destination. Each node in the path can explicitly ask the next hop for an acknowledgment. This mechanism is used to detect broken or unidirectional links;
4. If a node is no longer able to forward a packet to the next hop, it tries to solve the problem locally (Local Repair). In case it does not work, it sends a *Route Error* (RERR) to the originator of the message. The latter is then responsible for rebroadcasting a new RREQ.

Figure 3.1 depicts route construction between a source node (S) and a destination node (D). S starts by broadcasting a RREQ message with node D sets as the destination. Nodes in its vicinity receive the RREQ, construct a reverse route to the source, and broadcast the RREQ message. Upon reception of the RREQ message, the destination generates a RREP message in unicast. When node in charge of forwarding the RREP (as well as the source node) receives the RREP message, they construct the corresponding forward route which guarantee the bidirectionality of the route from source to destination. Differences between LOAD and LOADng can be found in Annex A.

RPL, being the routing protocol studied in that thesis will be described in details in the next section.

3.3 RPL

RPL has been defined in order to be Link-Layer agnostic i.e RPL is supposed to work on a wide variety of technologies such as Wireless or PLC network. RPL supposes that the predominant traffic is *Multipoint-to-Point* (MP2P) but it allows *Point-to-Multipoint* (P2MP) traffic, as well as *Point-to-Point* (P2P) traffic. RPL is part of the effort made by the *Internet Engineering Task Force* (IETF) to design an IPv6 architecture for LLN. As a companion, *IPv6 over Low power Wireless Personal Area Networks* (6LoWPAN) [MKHC07] defined the adaptations needed to use IPv6 in constrained networks. RPL is based on Distance Vector algorithms (the same family as RIP), and is designed to detect and react to loops. RPL is thus designed for applications typically seen in sensor networks – a central node (called a *border router* or *root node*) communicating with a set of sensors via fluctuating, low-bandwidth links. These characteristics correspond to the *Advanced Metering Infrastructure* (AMI) system (communication between *Data Concentrator* (DC) and Smart Meters (SMs)) and the technology of narrowband PLC NAN.

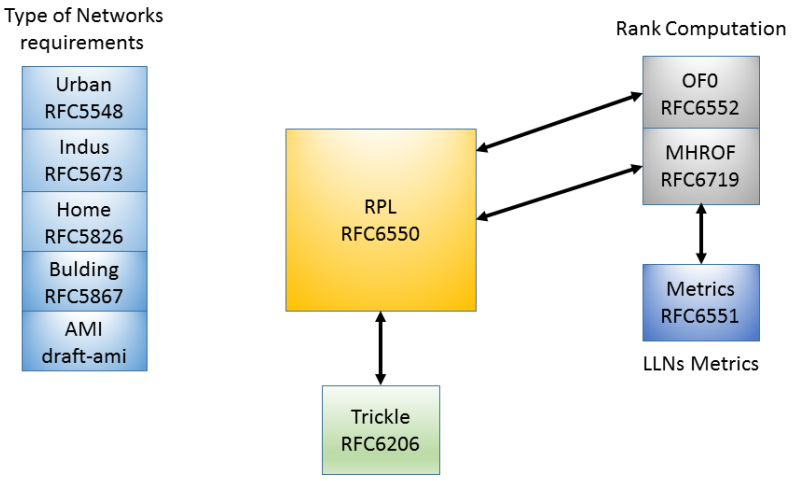


Figure 3.2: The RPL ecosystem.

Figure 3.2 shows the specification's work done by ROLL Working Group and their relationships. ROLL has designed the "ROLL Applicability Statement Template" [drac] in order to specify behavior and recommendations for specific network architecture. At present, four types of network architecture have been standardized:

- Urban Network [DWWB09];
- Industrial Networks [PTDP09];
- Home Networks [BBP10];
- Building Networks [MMRV10].

The organization in several standards regarding to application shows the constraint's heterogeneity regarding to the kind of network and application used. In order to define the requirements needed specifically for AMI, an applicability statement draft for AMI architecture has been proposed and is currently on the way to become an RFC [draa].

In RPL, in order to keep its agnostic approach, routing metrics are defined in a specific RFC [VKP+12]. RPL used a Gradient-based approach and the gradient used is the rank, which is a representation of the distance to the root. RPL transforms the metrics into rank by using *Objective Function* (OF) (presented in details in Section 3.3.3) . At present, two OFs are defined: *Objective Function Zero* (OF0) [Thu12] and *Minimum Rank with Hysteresis Objective Function* (MRHOF) [GL12]. In order to reduce signaling overhead due to the fact that RPL is a proactive protocol, RPL used Trickle algorithm [LCH+11].

3.3.1 Topology construction

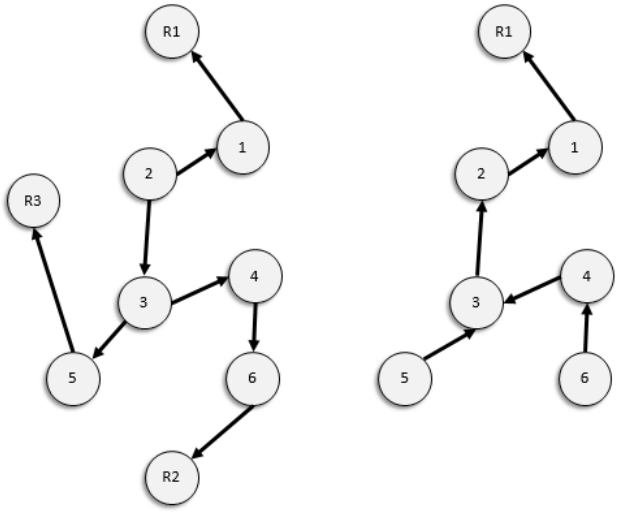


Figure 3.3: Examples of DAG and DODAG.

LLN, due to their intrinsics characteristic, do not have predefined topologies. RPL is in charge to discover and select nodes carefully in order to construct optimized topologies for traffic sent to the sink. To that purpose, RPL organizes topologies thanks to *Directed Acyclic Graph* (DAG). A DAG being a graph where the connections between the edges have a direction and a "non-circular" propriety i.e. moving from one node to another node following the edges guarantee to never encounter the same node a second time. A DAG root is a node that has no outgoing edge. Due to the acyclic nature of the graph, a DAG comprises at least one DAG

root. Figure 3.3(a) shows a DAG made of 6 nodes and 3 DAG root (R1, R2, and R3). To construct topologies, RPL use particular kind of DAG: the *Destination Oriented DAG* (DODAG) which is a DAG with only one DAG root i.e. the sink. Figure 3.3(b) depicts a DODAG made of 6 nodes with one DAG root (R1).

RPL uses three different values in order to organize a given topology:

- *RPLInstanceID*: identify a set of one or more DODAG. It is possible for a network to have several; *RPLInstanceID*. It has to be noted that all Destination Oriented DAGs (DODAGs) belonging to a *RPLInstanceID* must share the same OF;
- *DODAGID*: identify a particular DODAG in a *RPLInstanceID*. The combination of DODAG and *RPLInstanceID* identifies a DODAG in the network;
- *DODAGVersionNumber*: use to characterize the version of a given DODAG.

RPL establishes and maintains routes thanks to three types of messages: *DAG Information Object* (DIO), *DAG Information Solicitation* (DIS) and *Destination Advertisement Object* (DAO).

RPL works by installing upward routes first, and possibly downward routes.

3.3.1.1 Upward route formation

In a RPL network, at least one node is configured to act as a DAG root: the *RPL root*. This root broadcasts a DIO to its neighbors which are in turn broadcasting their own DIOs. DIO messages contain the rank of the sending node. The rank can be seen as a gradient which increases monotonically towards the edge of the network. The closer to the RPL root is situated a node, the smaller its rank is. A dedicated field – *DIO Rank* – is used by the receiving nodes, which upon receiving a DIO conjointly with a provided *Objective Function* (OF) compute their own rank. The OF defines how an observable metrics (such as hop-count or ETX) need to be minimized along the DODAG. Based on its own rank calculation, a node decides if it is going to use the DIO sender as a parent (e.g. install a route which uses the DIO sender on the way to the RPL root). Routes installed through the DIO mechanism (from the nodes to the root) are called *upward routes*. Once a node installs at least one upward route, it is said to have joined the DODAG.

Figure 3.4 depicts upward route construction using hop-count as metric. RPL root (Rank 1 Node) is the first one to send and propagate its DIO message. Neighbors in its coverage area are going to receive and processed the DIO. As the DIO is sent by the RPL Root, neighbors are going to add the RPL root as their preferred parent (nobody can be closer from the root than the root itself in term of hop-count) and to compute their Rank. The neighbors with Rank 2 are then going to send their own DIO and nodes in their vicinity are going to add node with Rank 2 as their preferred parent. These nodes will have a rank of 3. Once upward route

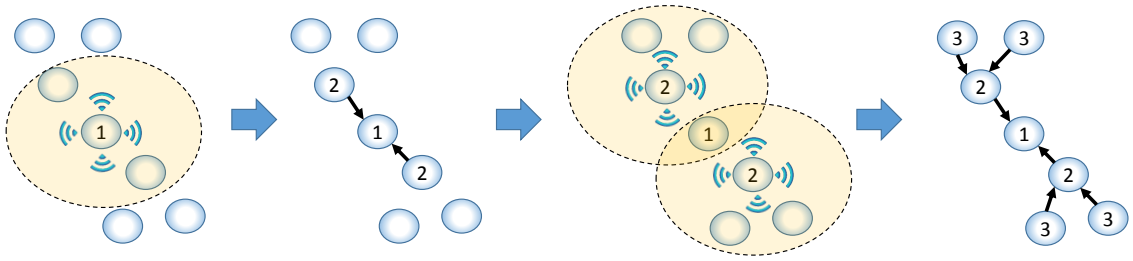


Figure 3.4: Upward Route Construction (Light Yellow Circle represents DIO transmission coverage area - Dark arrow represents Upward Routes - Number inside the circle represents the rank of a node).

construction is over, every node is the network is able to communicate with the RPL root.

The *DAG Information Solicitation* (DIS) message is used to solicit a DIO for a given RPL node (unicast DIS) or for the neighborhood (multicast DIS).

3.3.1.2 Downward route formation

Routes from the root to the nodes are called *downward routes* and are constructed and maintained with DAO messages. It has to be noted that downward routes are optional in RPL. DAO message contains the destinations reachable via a node, e.g. the IPv6 address of the Smart Meter. Two modes can be used for constructing downward routes: Storing and Non-Storing mode.

In *Storing mode*, the DAO messages are unicasted to the preferred parent which installs at reception of the DAO message the corresponding downward route. The DAOs propagate up to the RPL root through preferred parent in order to establish a complete downward path from the root to all destinations.

In *Non-Storing mode*, the intermediate nodes (i.e. preferred parent) do not install downward routes. Instead, the DAO message is sent to the RPL root with intermediary nodes just forwarding the DAO. When the RPL root needs to send a message to one (or more) nodes, it uses source routing to indicate the exact route of the packet.

It has to be noted that node can ask for an explicit End-to-End acknowledgment from the DAO recipient when sending a DAO message: the DAO ACK message.

Figure 3.5 presents downward route construction for Storing Mode for a given node (the green one) using hop-count as metric. The green Node is going to send its DAO which is in turn going to be received by its preferred parent which is going to install a downward route to the green Node. The node with rank 2 is then going to forward this DAO to its preferred parent, i.e the RPL root, which is in turn going to install a route to the green node.

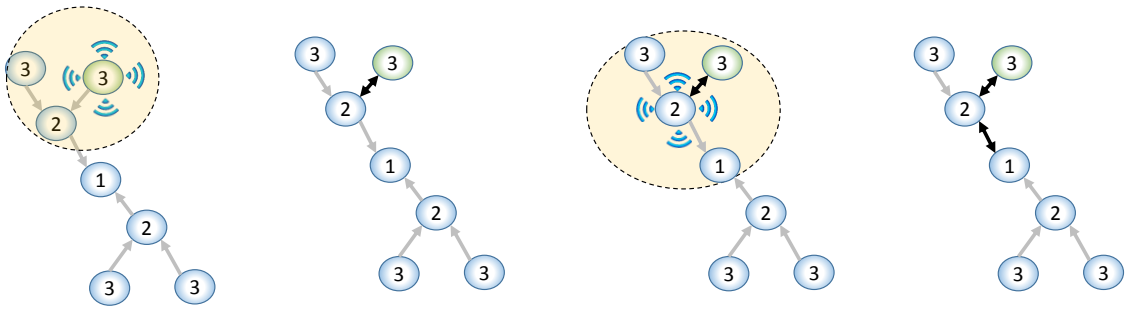


Figure 3.5: Downward Route Construction for Storing Mode (Green Circle represents the Node sending the first DAO - Light Yellow Circle represents DAO transmission coverage area - Light grey arrow represents Upward Routes and Double Dark Arrow represents bidirectional Routes regarding to the green node - Number inside the circle represents the rank of a node).

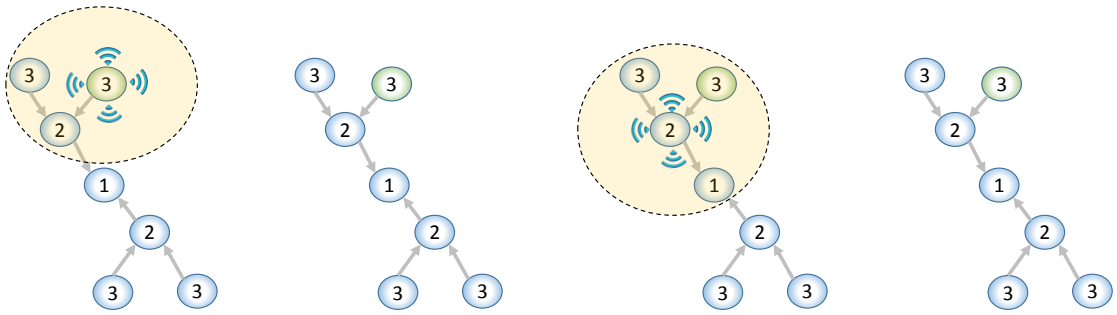


Figure 3.6: Downward Route Construction for Non-Storing Mode (Green Circle represents the Node sending the first DAO - Light Yellow Circle represents DAO transmission coverage area - Light grey arrow represents Upward Routes - Number inside the circle represents the rank of a node).

Figure 3.5 presents downward route construction for Non-Storing mode for a given node (the green one) using hop-count as a metric. Green Node is going to send its DAO which is in turn going to be receive by its preferred parent which is just going to forward it to the RPL root. At reception of the forwarded DAO, RPL root will handle the DAO message in order to be able to construct source routing to join the green node.

3.3.1.3 DODAG repair

Global and local repair are the mechanisms used to face network outage. Global repair is started by the RPL root by incrementing its version number and triggers a completely new DODAG topology by allowing nodes to choose a new position without being constrained by their rank in the old DODAG version.

RPL also allows a finest repair at a local level: the local repair. This mechanism

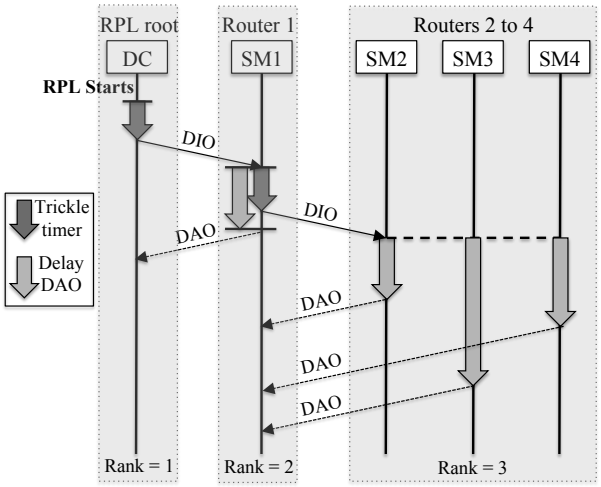


Figure 3.7: A RPL sequence diagram.

is used by a node which does not have anymore any potential parent and allows a node to choose a preferred parent without taking its own rank in consideration.

3.3.2 RPL messages timer

3.3.2.1 DIO: Trickle Algorithm

As RPL is a proactive protocol, DIOs are sent periodically to keep track of the state of the network. In order to minimize the number of DIO messages, a special timer algorithm called Trickle [LCH+11] makes sure that whenever the conditions are stable, the messages are sent scarcely. On the contrary, if the conditions evolve rapidly, the DIO messages are sent much more frequently.

3.3.2.2 DAO: DelayDAO

DAO emission is governed by an interval called *DelayDAO*. Each time a DAO has to be emitted by a node, a random value in the *DelayDAO* interval is going to be chosen before the DAO transmission. The RPL standard does not impose any specific value for this timer.

3.3.2.3 Topology construction at startup

Figure 3.7 shows a RPL control message sequence diagram when RPL starts. After Trickle timer, first DIO from RPL root reaches Router 1 which in turn is going to schedule its own DIO thanks to Trickle. In parallel, *DelayDAO* is armed and once expired, triggers the sending of the DAO to the RPL root. Once Trickle

timer expires for Router 1, it sends its DIO that Routers 2, 3, 4 are going to receive simultaneously. They arm the *DelayDAO* timer and send their corresponding DAOs.

3.3.3 Objective Function

The *Objective Function* (OF) plays a major role for RPL. by allowing to:

- Compute the node's rank i.e the distance to the root;
- Define how to select and optimize routes within a RPL Instance.

In order to propagate the OF to use inside a given RPL instance, the root includes an *Objective Code Point* (OCP) in its DIO message. ROLL working group has defined so far two OFs: *Objective Function Zero* (OF0) and *Minimum Rank with Hysteresis Objective Function* (MRHOF):

3.3.3.1 OF0

OF0 [Thu12], sometimes referred as a weighted hop-count function, works by computing the rank based on the addition of a scalar value (normalized between 1 and 9 for expressing the link properties with 1: excellent and 9: very poor) to the rank of its preferred parent (announced through DIO message). The scalar value can be any kind of metric (see Section 3.3.4).

The rank computation is given by Algorithm 1. The rank of a node is computed by adding the preferred parent rank to the rank increase. The rank increase being the expression of the link property as stated in Algorithm 1.

Algorithm 1: Rank Computation for OF0

$R(N) = R(P) + rank\_increase$
$rank\_increase = (Rf * Sp + Sr) * MinHopRankIncrease$
where:

- $R(p)$: preferred Parent's rank
- Sp: $step\_of\_rank$ The expression of the link properties normalized between 1 and 9. It has to be noted that [Thu12] does not define how to normalize a given metric as it is implementation dependent.
- Sr: $stretch\_of\_rank$ the maximum augmentation to the $step\_of\_rank$ of a preferred parent to allow the selection of an additional feasible successor. If none is configured to the device, then the $step\_of\_rank$ is not stretched.
- Rf: $rank\_factor$: a factor used to increase the importance of the link properties in the $rank\_increase$ computation

MinHopRankIncrease plays a major role in rank computation as it reflects the

impact of the metric on rank increase: the bigger it is, the higher is the influence of a given metric on rank increase. Being a multiplying factor, the choice of *MinHopRankIncrease* strongly influences the maximum number of hops in the network as it constraints by nature the rank. *MinHopRankIncrease* is also used to compare rank during parent process selection. Indeed, RPL rank can be seen a fixed-point notation where radix point's position between the integer part and the fractional part is determined by *MinHopRankIncrease*. During rank comparison, Algorithm 2 is used.

Algorithm 2: Rank Comparison

R1 and R2 being respectively the rank of Node 1 and Node 2
$DAGRank_{(rank)} = floor(rank/MinHopRankIncrease)$
if $(DAGRank_{(R1)} < DAGRank_{(R2)})$ **then**
  Node 1 has a Rank less than the Rank of a Node 2
else if $(DAGRank_{(R1)} > DAGRank_{(R2)})$ **then**
  Node 1 has a Rank greater than the Rank of a Node 2
else
  Node 1 has a Rank equal to the Rank of a Node 2
end if

Parents selection followed several rules but the most important is that the selected parent must be the one that causes the lesser resulting rank for the node.

3.3.3.2 MRHOF

Minimum Rank with Hysteresis Objective Function (MRHOF) [GL12] aims to optimize path that minimize a metric but avoid too frequent path changes for too-small metric variations by introducing hysteresis. MRHOF works with additive metrics along a route, and the corresponding metric are disseminated by the DIO messages thanks to the DIO metric container option.

For the rank computation, MRHOF introduces the notion of path cost that quantifies the property of the path to the RPL root regarding to the metric used. The path cost is obtained by summing up the link metric cost regarding to a parent with the path cost advertised by the parent. The way to turn a path cost into a rank is metric dependent as stated in Algorithm 3.

In order to select parents, MRHOF introduces an hysteresis function that can be expressed by Algorithm 10.

OF's goal is to define how to turn a metric into a rank. Next section presents the usable metrics defined by ROLL working-group.

Algorithm 3: Rank Computation for MRHOF

$path_{cost} = parent_{path\_cost} + link\_cost$
$rank = func(path_{cost})$
where $link\_cost$ is the cost associated with the parent's link regarding to the selected metric and $parent_{path\_cost}$ is advertised by the parent and represents the $path\_cost$ of the parent itself. The way to turn the $path\_cost$ into a rank depends from the chosen metric and is defined in [GL12].

Algorithm 4: MRHOF Hysteresis function

$P1$ and $P2$ being respectively the path cost to Parent 1 and Parent 2
$P1$ is the current best parent and $P2$ is a candidate parent
if $P1_{path\_cost} + PARENT\_SWITCH\_THRESHOLD > P2_{path\_cost}$ **then**
  Switch to $P2$ as a preferred parent
else
  Keep $P1$ as a preferred parent
end if
where $PARENT\_SWITCH\_THRESHOLD$ is the hysteresis function i.e. the minimum difference between the cost of the path through the preferred parent and the cost path of a candidate parent in order to trigger the selection of a new preferred parent

3.3.4 Metrics

[VKP+12] defines two kinds of routing metrics categories that can be used for path calculations.

- Node Metrics: takes into account attributes relative to the node;
- Link Metrics: uses link's attribute e.g throughput, latency, Link Quality Level (LQL), or Expected Transmission Count (ETX).

Node Metrics can be:

- State and Attribute: provides information on node characteristics such as workload that can be expressed thanks to CPU overload, node's memory, etc.;
- Energy: represents node's power sources or remaining energy;
- Hop-Count: number of traversed nodes along the path (regarding to the root).

Link Metrics can be:

- Throughput: range of throughput that their links can handle in addition to the currently available throughput;
- Latency: the duration for a packet to arrive at a destination once sent;
- Reliability: Either discrete (between 0 and 7) to express the Link Quality Level Reliability Metric or expressed as the *Expected Transmission Count* (ETX)

OS	Mode	OF	Metric
TinyOS RPL	Storing	OF0 & MRHOF	Hop-Count & ETX
ContikiRPL	Storing	OF0 & MRHOF	Hop-Count & ETX & Energy
SimpleRPL (Linux)	Storing	OF0	Hop-Count
RIOT	Non-Storing & Storing	OF0 & MRHOF	Hop-Count & ETX
OpenWSN	Non-Storing	OF0 & MRHOF	Hop-Count & ETX
Unstrung (Linux)	Non-Storing & Storing	OF0 & MRHOF	Hop-Count & ETX

Table 3.1: RPL Operating Systems implementation main characteristics.

i.e the number of needed transmission of a packet to arrive at its destination;
- Color: An administrative link constraint (which may be either static or dynamically adjusted) used to avoid or attract some specific links for specific traffic types.

3.3.5 RPL Implementations

A wide variety of implementations are available for different *Operating System* (OS). Table 3.1 summarizes their functionalities:

Several implementations are also available for simulation environment such as *NS-2*, *OMNET++*, *JSIM*, *Qualnet*, or *WSNet*. It has to be noted that *ContikiOS* offers a simulation environment called *COOJA*.

3.4 RPL IN THE LITERATURE

The adaptations and new mechanisms we proposed for RPL for SG networks were based on issues identified via analysis and evaluation of multiple scenarios from theoretical point of view, and in simulation and testbed executions.

In order to identify the potential problems, and the available solutions, we performed an in-depth study of the state of the art. This section presents the most relevant works found in the literature.

Table 3.2 summarizes these studies, which we selected either for their particular relevance to RPL (performance evaluations, new proposals, comparisons with other routing protocols, etc.), or for their pertinence to RPL in PLC environment. We

can observe from this table that:

- While RPL has been widely studied for *Wireless Sensor Network* (WSN) environment, few studies are focused on RPL's behavior with PLC;
- There is a predominant usage of Contiki RPL implementation when it comes to studying RPL;
- RPL is often studied by simulation;
- The scale of the scenario, be it by simulation or in a real-world testbed, varies considerably – from few nodes to more than thousand. The general case appears to be in middle-scale environment i.e. around 100 nodes;
- ETX is considered as the default metric for RPL as shown by the usage of this metric in all presented studies.

3.4.1 PLC and RPL studies

Chauvenet *et al.* performed the very first trial of RPL usage in PLC environment for Smart Metering [CTGC+10]. The authors proposed a communication stack for PLC based on open standards by adapting IEEE 802.15.4 protocol with 6LoWPAN to PLC environment. They tested it on real-world testbed, with *ContikiOS*-based nodes, and showed a gain of 45% in the latency by using their own stack with activated 6LoWPAN.

Ben Saad *et al.* implemented a PLC module for the *ContikiOS COOJA* simulator and a RPL module for *WSNet* [SCT11]. The performance of RPL was analysed in two scenarios. The first one focused on WSN and analyzed the effect of *sink* mobility on energy consumption (i.e. RPL root mobility). They concluded that sink mobility allows to save energy compared to a static sink. The second scenario compared a real PLC testbed (based on [CTGC+10]) with the results of their PLC module in *COOJA* for 6 nodes and one RPL root. The results obtained by simulation show better performance than the one observed on the real testbed.

Pignolet *et al.* studied RPL's performance in Medium Voltage realistic topology [PRDK12]. They proposed a *Signal-To-Noise Interference-Ratio* (SINR) model to model the physical layer characteristics over medium voltage power lines, and implemented the IEEE P1901.2 in Contiki. The results were obtained from *COOJA*-based Contiki simulations.

Balmau *et al.* extends ContikiOS in order to support several communication interfaces and more notably PLC [BDK+14]. They evaluated RPL's behavior on a Medium Voltage realistic Smart-Grid topology using RPL with ETX metric and two PLC interfaces. They showed that Packet Success Ratio decreases significantly with distance (90% for less than 2000m and less than 50% for distances over 6000m). Conversely, latency is increasing with distance (around 10ms for distance less than 2000m and less than 60ms for distance around 6000m). In a simulation testbed of 93 Nodes, they concluded that Packet Success Rate and latency are directly related

Implementation	Reference	Environment		Simulation	Scale	RPL Metric		
		WSN	PLC			Hop-Count	ETX	Others
Contiki	[ABC14a]	✓		✓	150		✓	
	[GFBK11]	✓		✓	70		✓	RSSI
	[VTD13]	✓		✓	25		✓	
	[AGBC11a]	✓		✓	100		✓	
	[ABC+14b]	✓		✓	150		✓	
	[CLCL13]	✓		✓	6		✓	Remaining Energy
	[DDB12]	✓		✓	100		✓	
	[ABC13]	✓		✓	150		✓	
	[ABC12]	✓		✓	150		✓	
	[GK14]	✓		✓	100		✓	Traffic load/packet losses
	[LHG13]	✓			50		✓	
	[GKPG14]	✓		✓	25	✓	✓	
	[DCTS12]	✓		✓	49		✓	
	[BBCF13]	✓			25		✓	
	[OPOP12]	✓			21		✓	
	[HM13]	✓			250		✓	
	[PRDK12]		✓	✓	16		✓	
	[BDK+14]		✓	✓	100		✓	
	[CTGC+10]		✓		5		✓	
	[SCT11]		✓	✓	7		✓	
TinyOS	[GKPG14]	✓		✓	25	✓	✓	
WSNet	[SCT11]	✓		✓	1600		✓	
	[ITN13]	✓		✓	100	✓	✓	LQI
OMNET	[IA13]	✓		✓	50		✓	
	[TdO13]	✓		✓	75		✓	
ns-2	[YC13]	✓		✓	500		✓	

Table 3.2: RPL studies depending on Implementation used.

	Performances analysed					
References	E2E delay	Overhead	PDR	Throughput	Route Formation	Stability
[AGBC11a]	✓	✓		✓		
[ABC13]	✓	✓	✓			
[ABC12]	✓		✓			
[ABC+14b]	✓		✓			
[GFBK11]			✓			
[BDK+14]	✓		✓			
[SCT11]	✓			✓		
[GK14]					✓	
[GKPG14]	✓					
[HM13]		✓				
[ITN13]			✓			✓

Table 3.3: RPL performances analyzed.

to traffic load and distance.

To the best of our knowledge, these are the only relevant studies for RPL in a PLC environment. The limited number of studies shows the lack of available material allowing to construct a complete picture of the performance of RPL in the context of PLC-based AMI.

There are several reasons which lead to this scarcity on the topic. On one hand, RPL is a relatively new protocol with limited number of available implementations – real-world or for simulations. On the other hand, narrowband PLC technologies, such as the ones envisioned for AMI, are also very new, with even fewer realistic physical layer models. The combination of the two makes the subject even more challenging. This is also the reason RPL was studied in much greater lengths in the context of Wireless Sensor Network, as presented in the following subsection.

3.4.2 RPL and WSN

Compared to PLC environment, RPL has been massively studied in WSN due to its usage precedence. We classified existing works in two main sections:

- Performances: Analysis of RPL's behavior compared to itself or to other protocols;
- Improvements to RPL: New metrics, or protocol improvements in order to guarantee better performance.

References	Comparison routing protocols				Results
	LOAD	LOADng	CTP	Geographical routing	
[IA13]	✓			✓	RPL++ LOAD -
[TdO13]		✓			RPL + LOAD -
[YC13]		✓			RPL- LOAD++
[VTD13]		✓			RPL+ LOAD-
[DCTS12]			✓		RPL+ Geographical-

Table 3.4: RPL performances compared to other routing protocols under study.

3.4.2.1 Performances

RPL's performance was studied in different ways. While some authors base their studies only on a packet forwarding approach (*Packet Delivery Ratio* (PDR), *End-to-End* (E2E) delay, etc.), others try to measure RPL's performance from the perspective of DODAG construction process (stability, DAG construction, etc.). Table 3.3 outlines the presented papers and the performance evaluations. From this table, we can observe the following:

- E2E delay and PDR are the most-frequently used metrics to evaluate RPL;
- Signaling overhead is an important value for analyzing in RPL, as it is a proactive protocol. However, RPL performance can be expressed by other means depending on the goal. For example, stability (i.e. the number of DODAG topology reconfigurations) is an interesting indicator to measure the efficiency of a given RPL metric.

Another approach to analyze RPL performance is to compare it to other routing protocols. This approach is interesting but presents several difficulties:

- Routing protocols' performances can be widely influenced by the protocol configuration, e.g. changing the trickle timer value in RPL radically modifies the generated overhead;
- The used implementation has to be correctly implemented, i.e. must comply with the most recent version of the standard (or the draft) of the protocol, as well as be implemented with the same level of accuracy. A bug in the code, or a missing feature can heavily penalize the performance of a protocol, and the probability of this happening rises with the complexity of the protocol, RPL being on the high-complexity end of the spectrum;
- The chosen scenario must reflect the environment under study, which should be defined a priori. For example, low data traffic patterns would advantage reactive routing protocols performances' against proactive ones in the ratio overhead/data.

Table 3.4 shows the diversity of results that can be obtained when comparing two routing protocols. From this table, we can observe that:

- When it comes to comparing two routing protocols, it is not rare to find contradictory results;
- LOAD and LOADng seem good candidate to compare with RPL protocols as apparently conflicting results can be obtained.

In [AGBC11a], Accettura *et al.* studies RPL's behavior in a WSN of 100 nodes. Their simulation shows that RPL can ensure a fast network convergence but that the generated overhead should be reduced (overhead representing 75% in steady-state for 100 nodes). RPL's signaling overhead importance has also been tackled in [IA13], [VTD13] and [YC13]. Particularly, [TdO13] highlights the fact that RPL signaling and specifically DAO messages can lead to congestions.

[HM13] investigated RPL's behavior in dense network. They observed that RPL can guarantee a strong path stability despite the instability of the physical topology. They also demonstrated that RPL PDR is quite low for very dense networks.

[GKPG14] compared MRHOF and OF0 *Objective Function* (OF) performances. They showed that MRHOF allows better performance in term of PDR due to the fact that OF0 considers only the best parent link quality while MRHOF takes into account the quality of the entire path. Further analyzes of RPL with MRHOF are made by Ancillotti *et al.*, who for their part, focused in [ABC13] on studying the role of RPL for Smart Grid communications and more particularly in AMI. They showed that few nodes in the network can experience high loss rate due to inefficient routing decision. They explained that phenomena in details in [ABC12] by the fact that RPL could select an upward route that includes a low-quality link because RPL lacks a complete knowledge of link qualities, i.e. only the best parent's link quality is evaluated. [DDB12] also highlights parent's suboptimal selection due to Contiki's conservative approach when initializing the metric value at the time the link quality with the parent is unknown. [ITN13] extends the study by analyzing the network instability for three metrics: hop-count, ETX and LQI. While hop-count leads to shorter path with poorer link-quality, ETX provokes high instability in the network due to its reactivity to link-quality change.

Several papers focus on the comparison of RPL against other protocols. For example, [YC13] compared LOADng and RPL. They concluded that LOADng operates in a better way for WSN environment in terms of PDR, signaling overhead, and E2E delay. The opposite has been demonstrated in [TdO13] where the authors put the emphasis on the choices that were made for studying RPL in [YC13]. They also raise the question of a hybrid approach (proactive and reactive). [LHG13] defines such approach by using LOADng instead of RPL to construct downward routes. [VTD13] compares RPL and LOADng protocols. They showed that RPL allows better performances in term of delays, overhead and memory. [IA13] shows that although LOAD is designed for LLN, it does not perform well in both route formation time and E2E delay compared to RPL. [DCTS12] compares RPL and the Collection Tree Protocol (CTP). They demonstrated that RPL performs better in

	Link Estimation			New Metric		Opportunistic Routing
	Hybrid	Active	Passive	Energy	Composite	
References	[ABC12]	[ABC+14b]	[DDB12]	[CLCL13]	[GK14]	[GFBK11]

Table 3.5: RPL improvements.

term of latency and convergence time than CTP.

3.4.2.2 Improvements

In order to improve RPL's behavior, enhancements have been proposed to RPL protocol. Table 3.5 proposes a classification of some of these improvements.

Regarding to link-estimation, to overcome the aforementioned problem described in [ABC13], Ancillotti *et al.* proposed modifications to RPL specially focused on Contiki [ABC12]. By changing some of Contiki's behavior (mainly routing and neighbor table management) and by switching from a conservative to a hybrid (active+passive) approach for parent link quality estimation, they outperformed Contiki's RPL performance Packet Delivery Rate by 200%. In order to reduce overhead induced by a permanent probing mechanism, Ancillotti *et al.* introduced the *Trickle-L2* mechanism [ABC+14b]. The goal of this improvement is to enable a faster DODAG construction by delaying the bootstap process until a certain link quality is reached. To do so, probe DIOs are emitted thanks to Trickle in order to allow neighboring nodes to estimate the link quality. They showed that the Trickle L2 mechanism allows better convergence at the price of a small overhead. [DDB12] proposed a new mechanism to estimate link quality: passive optimistic probing. Instead of considering a new neighbor having a bad link quality, they consider that this new neighbor is having the best link quality. It allows to test more neighbors and not to stick to an acceptable one. They showed that at the price of a bigger number of parent change, the number of retransmission is lowered.

As our work focus in Smart Grid environment, the device are not power-constrained but an entire field of study is dedicated to design new metrics that take into account energy (remaining energy of the node, reducing energy's bottleneck, etc.). In [CLCL13], Chang *et al.* introduced a new metric in order to take into account not only ETX but also the remaining energy metric. They showed that their new metric allows to increase the network lifetime by 12%.

Some original approaches have also been proposed in order to improve RPL. For example, opportunistic routing is popular in WSN self-organizing networks. Thus, [GFBK11] designed an opportunistic version of RPL called ORPL. It takes advantage of the fact that most of the time a node is having several potential parents. Instead of forwarding the frame only to the best parent, the frame is forwarded to

all potential parents. Compared to RPL, ORPL shows better performances in term of PDR and number of retransmissions.

[GK14] introduced a new objective Function: OF-FL (Objective Function Fuzzy Logic) in order to take into account several metrics by using fuzzy logic. This new OF allows to obtain better E2E delay, network lifetime and PDR.

As shown in this section, RPL has been widely studied in WSN. One constant is that the community seeks to improve RPL for their specific usage. This shows the need for us to to analyze the performance of RPL for the context of PLC-based AMI and if necessary, propose new solutions specially tailored for IEEE P1901.2 environment.

3.5 Conclusion

3

In this chapter, we introduced RPL – the proactive routing protocol for LLN. We showed that because of RPL's link-layer agnostic nature, RPL needs to be adapted and optimized specifically for the environment in which it operates. Because of Advanced Metering Infrastructure's traffic patterns, and the intrinsic characteristics of narrowband PLC, RPL needs to be carefully tuned in order to work optimally in this kind of environments. To that purpose, simulation allows to perform optimization testing at a lower cost, which is one of the contributions of this thesis. The next chapter presents the simulator that we implemented in the context of this thesis.

4 Simulator Overview

As we highlighted in Chapter 3, few of the existing works are concerned with RPL's performance in PLC environment and even less in NB PLC. This motivated our work to develop a new simulator that implements a full IEEE P1901.2 stack.

In the following chapter, we present an overview of the selected simulator functionalities and design in Section 4.1. The choices that we made for our simulator development are detailed in Section 4.2. We then describe the physical model that we designed and implemented in our simulator in Section 4.3. Finally, a systematic validation of our simulator against a real-testbed in Section 4.4 in order to guarantee confidence in results obtained later in this thesis.

4.1 Network Simulator choices

Several popular network simulators exist, each having its strengths and weaknesses, such as *OMNET++*, *ns2*, *ns3*, *WSNet*. Our simulation model was implemented in OPNET, which was selected as a preferred tool in terms of its industry-wide acceptance, existing physical libraries, MAC source code availability and graphical presentation. *OPNET* uses a proprietary *Proto-C* approach, which consists of:

- State transition diagrams;
- Complete C and C++ programming language;
- Library of *OPNET* Kernel Procedures.

The usage of Proto-C and most particulary the OPNET kernel library allow easier development with optimized simulation run.

Concerning RPL, the protocol was designed to cover a wide variety of link layers. In that purpose, IETF RPL standard leave many parameters up to the implementer. At present, at least six RPL implementations are available as shown in Table 3.1. We decided to base our simulator RPL implementation on Contiki's one. Indeed, Contiki is used in most of the studies performed on RPL and is the "de facto" reference implementation. This choice allows us to check if some weaknesses attributed to RPL were due to RPL or Contiki Team implementation's choices. ContikiRPL is based on the RPL RFC and offers the possibility to use both *Objective Function Zero* (OF0) and *Minimum Rank with Hysteresis Objective Function* (MRHOF)

with ETX, hop-count or energy metric.

4.2 Simulator's overview

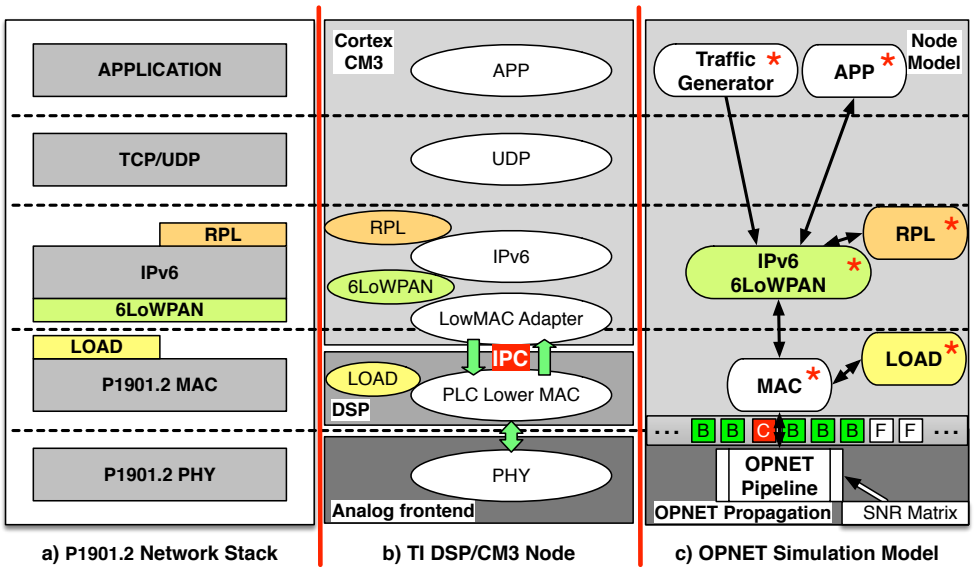


Figure 4.1: An overview of the complete architecture.

OPNET implements devices with a *Node Model* (NM). Fig. 4.1 shows the NMs correspondence to the P1901.2 network stack and the testbed implementation. Each NMs consists of several *Process Model* (PM) that can communicate together, with separate networking layers being implemented through different PM. The physical model (Section 4.3) is used in MAC's PM to check the *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA) channel state, and to compute the *Signal Noise Ratio* (SNR) (average or per sub-band) in the pipeline stage.

The model we developed implements a complete IEEE P1901.2 PLC device including:

- PHY and MAC layer;
- CSMA/CA Channel;
- RPL/LOAD/LOADng;
- 6LoWPAN.

4.3 Physical Model

4.3.1 Overview

The simulator has to be efficient, capable of simulating in the order of 1000 nodes required to obtain results for even the most dense SM deployments. OPNET, an

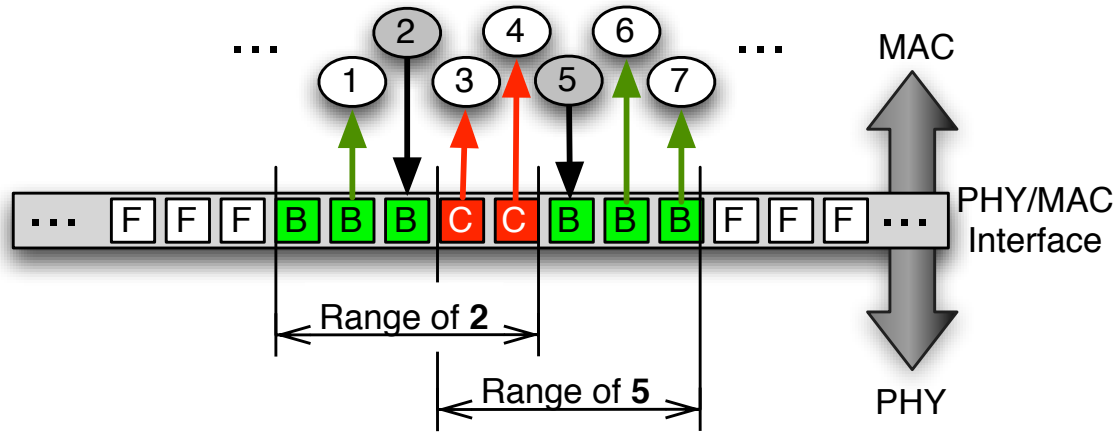


Figure 4.2: PHY/MAC interface. The numbers **1**, **2**, **3**, ..., **7** represent Smart Meters. **2** and **5** are emitting simultaneously, and their transmission ranges by a simplified internal model, or by a realistic external one. Nodes **1**, **6** and **7** receive the information correctly (and their medium is *B*usy), while **3** and **4** are incapable of decoding the information as the PLC link at their location is in *C*ollision. All others are *F*ree.

event-driven simulator, was chosen as the basis of our development. We modeled the physical channel with a mathematical model, which we use to determine the error rate and other parameters such as *Tone-Map* (TM). The core of the simulator is a Finite State Machine (FSM) representing the channel behavior.

The topology of the PLC network has to be as flexible as possible to handle the large variety of environments we want to simulate. We created an external tool, which based on a generic graph generates a two-dimensional matrix, representing the distances between each pair of nodes. This tool is part of a set of supporting tools we developed for *OPNET* to simulate the PLC communication.

The model we developed under *OPNET* takes as input the two-dimensional distance matrix. Based on the distance matrix, an SNR matrix is computed. The matrix $C = c_{ijk}$ represents the SNR for every pair of nodes i and j on every group of channels k. The SNR matrix $C = \{c_{ijk}\}$ is (possibly) asymmetric, thus allowing the simulation of non-isotropic signal propagation. During the simulations, the OPNET model uses the C matrix to determine the transmission range, the bit-error-rate (BER) for all available modulations and for all subcarrier groups. This is in turn used to dynamically calculate the Tone-Map and the neighbors of a node.

Since the calculation of all these characteristics can prove to be extremely time-consuming for large topologies and long simulations, we introduced an interface providing the MAC layer with a macroscopic view of the physical layer. The interface layer (Fig. 4.2) has a limited number of macro (MAC-layer) states indicating the state of the medium at each node, as well as the modulation and the sub-bands to be used by a node to reach its neighbors. The link state is modeled as a vector L

where L_i indicates the link status for node i. The link at each node can be:

- F (Free) – There is no ongoing transmission. CSMA/CA will not sense any carrier and will allow the node to start transmitting after the expiration of the backoff period.
- U (Unknown) – There is an ongoing transmission but the channel is considered free. CSMA/CA will not sense the carrier and will allow transmission, thus generating a collision. This state is necessary in order to model collisions dues to propagation delays. The state transitions from U to B after the maximum propagation time elapses. It may also transition to C if a collision occurs.
- B (Busy) – There is an ongoing transmission and the channel is occupied. CSMA/CA will sense the carrier and will prevent the node from sending any data (backoff).
- C (Collision) – There are two or more ongoing transmissions at this node's position. If the node is sending data it will continue to do so as it cannot sense the collision (instead, a missing ACK will trigger retransmission). The frame will be silently discarded by the PHY layer if this is not the sender node. This state may occur whenever there is a hidden node phenomenon or a collision has occurred due to propagation delays.

A sending node changes the link state of its neighbors – the nodes in its transmission range. Figure 4.3 presents the possible transitions for the link of our CSMA/CA channel model.

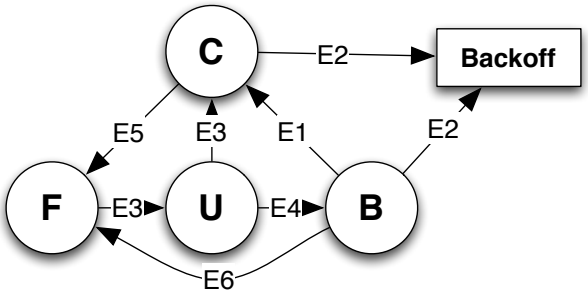


Figure 4.3: State transitions for CSMA/CA model. E1: Neighbor sending, E2: Node sending, E3: E1 or E2, E4: Propagation time, E5: Collisions end, E6: Transmission end.

The granularity can be adjusted by varying the frequency of updating the macro states from the physical layer information. Moreover, we can update the SNR matrix during the simulation. We can thus have situations where the characteristics of the medium change drastically, e.g. a line getting damaged, or a big load added to the circuit. In addition, it is possible to consider the C state as one in which some communications are possible with a higher BER. Currently we associate a collision with a frame loss. In [RLP+], we show that this simplification does not interfere with the validity of the simulations.

4.3.2 SNR computation

The SNR is computed based on the power of transmission, the linear attenuation (regarding to distance) and the noise (obtained from a noise database). Equation 4.1 shows the SNR computation.

$$SNR = ATL - ATT - ATN \tag{4.1}$$

where ATL is the average transmission level depending on the case, i.e.:

- *Average Preamble Transmission Level* (APTL): Used in packet reception to detect if the preamble can be decoded;
- *Average Data Transmission Level* (ADTL): Used in packet reception to detect if the data can be decoded;
- *Average Sub-band Transmission Level* (ASTL): Used for Tone-Map detection procedure.

Average Total Noise (ATN) is made of a noise database computed based on a *MATLAB* model while ATT represents the attenuation between a pair of nodes and is computed linearly regarding to distance from Equation 4.2. This equation is based on a simplification of the model for multipath signal propagation in PLC proposed in [ZD02].

$$ATN = 10 \log_{10} e^{-(a_0 + a_1 f_{mid}^{\gamma})\, d} \tag{4.2}$$

where d is the distance between the receiver and the transmitter and $f_{mid} = 63$ kHz is the central frequency of the CENELEC A PLC bandwidth.

This model assumes that:

- There is no impact of the frequency on the loss when the PLC bandwidth is considered;
- The loss is rapidly decreasing with the distance.

This model provides realistic results with low computational complexity approach to emulating the narrowband PLC channel behavior. Having a micro-second level simulation of the channel, over a much more detailed power line topology information is an extremely challenging task, which is unfit for big scale simulations. In addition, the latter approach requires the detailed specification of the specific power line topology (e.g. length of cables, the metal composition, impedance, circumference, type of connection between the cables, interrupters, plugged-in electrical devices) – a task worthy of dedicated research efforts.

The SNR is used for the Tone-Map procedure as well as the error computation.

4.3.2.1 Tone-Map procedure

The Tone-Map procedure is the process that determines which modulation and which sub-bands can be used for communicating with a node. As stated in Section 2.3.3, IEEE P1901.2 CENELEC A band is made of six sub-bands of six tones.

The SNR can be computed per sub-band. Thus, it is possible to know which sub-band must be ON or OFF depending on the modulation to use as well as on the targeted objective – for example maximize the throughput or avoid fragmentation. In our implementation, we used the Tone-Map selection in order to maximize throughput.

Algorithm 5 shows computation of the throughput estimation for a given modulation depending on the SNR per sub-band. Four different modulations can be used: ROBO, DBPSK, DQPSK and D8PSK.

Algorithm 5: Thoughput Computation

$MAX\_MOD = 4$
$MAX\_SUB\_BAND = 6$
for $(i = 0; i < MAX\_MOD; i++)$ **do**
  for $(j = 0; j < MAX\_SUB\_BAND; j++)$ **do**
    if $SNR[j] > Threshold[Index]$ **then**
      $Throughput[i] = Throughput[i] + Capacity[i]$
    end if
  end for
end for

The selection of the modulation is performed by Algorithm 6. Its goal is to maximize the throughput.

Algorithm 6: Modulation Computation

$MAX = Throughput[0]$
$indexMax = 0$
$MAX\_MOD = 4$
for $(i = 1; i < MAX\_MOD; i++)$ **do**
  if (MAX < Throughput[i]) **then**
    MAX = Throughput[i]
    IndexMax= i
  end if
end for
Tone Map Modulation = Modulation[IndexMax]

Finally, the activated sub-bands are computed by Algorithm 7.

Algorithm 7: Sub-band selection

```
SubBand[0... MAX_SUB_BAND - 1] = 0...0
for (i = MAX_SUB_BAND - 1 ... 0 ) do
  if (SNR[i] >= Threshold_1[IndexMax]) then
    Sub Band[i] = 1 : ON
  else
    Sub Band[i] = 0 : OFF
  end if
end for
```

4.3.3 Errors Computation

Error computation permits to decide if a frame can be decoded by a receiving node. In that purpose, SNR Vs BER curves based on a Matlab models are used in order to obtain a BER corresponding to an SNR.

4.4 Simulator's validation

In order to validate the developed simulator, we use a real-world testbed allowing us to construct several relevant SMs deployment scenarios (Figure 4.4). The testbed consist of nine IEEE P1901.2 nodes – Texas Instruments Reference Design kits. The kits have a dual-processor architecture, with a *Digital Signal Processor* (DSP) for the networking functions, and a Cortex M3 processor for the routing protocols and the application development. The kits implement the complete IEEE P1901.2 specification (PHY, MAC, LOAD) in the DSP. However, no implementation of RPL was available. Thus, we developed a full RPL implementation in the Cortex M3 core based on the reference stack from Contiki 2.5. As Cortex M3 is using FreeRTOS Operating System, a full port of Contiki IPv6 Stack has been done to FreeRTOS. Fig. 4.1b shows the protocol implementation point (DSP or Cortex). RPL used for the platform is using Objective Function 0 [Thu12] with hop-count as a metric.

The 9 nodes have been setup in the following configuration:

- One *Data Concentrator* (DC) interacting with the meters;
- Six SM reporting to the DC;
- Two sniffer nodes allowing the observation and analysis of the traffic on the line. A modified version of Wireshark is used for collecting the traces;
- *Objective Function Zero* (OF0) is used with hop-count as a metric.

The construction of the deployment scenarios is achieved by inserting signal attenuators to the power lines connecting the nodes. Each $40dB$ attenuator has an impedance of 50Ω. Selecting the meter's lowest transmission power, two power meters communicate through one attenuator, but not through two consecutive ones,

equivalent to 200m in the simulator.

4.4.1 Methodology

In this section, we present the validation of the simulator against the performance observed in the real-world testbed. The validation scenarios have been carefully selected in order to represent some of the most frequently met real-world situations, and address *Urban*, *Rural* and *Mixed* topologies (Figure 4.4). All scenarios contain a Concentrator (DC) and six Smart Meters (SM) as shown in Fig. 4.4.

In order to validate the simulator and the developed models, we chose a set of representative scenarios (topology, traffic patterns, etc.), which were executed on the testbed and in the simulator. A set of metrics was collected in both contexts and the resulting values analyzed for statistical resemblance.

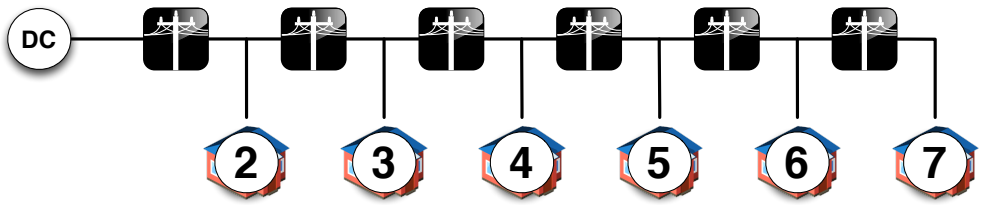
The validations were carried over the behavior of two fundamentally different routing protocols (RPL and LOAD) and their influence on the data plane. The data traffic patterns presented in this paper correspond to typical interactive Smart Meter reading, where the DC sends requests to the meters, which respond immediately. Specifically, the DC sends UDP datagrams of payload 50 bytes to every Smart Meter every 30 seconds. The Smart Meter responds with the same payload. We selected the metrics which are most representative for the performance of the protocols, and which validate essential parts of the simulator. The metrics are the following:

- End-to-End delay (E2E): round-trip time for a data request/response;
- Route Formation Time (RF): time and volume of signaling data needed to establish all routes between DC and SMs;
- Route Maintenance Signaling Traffic (RM): volume of signaling data needed to maintain the topology.

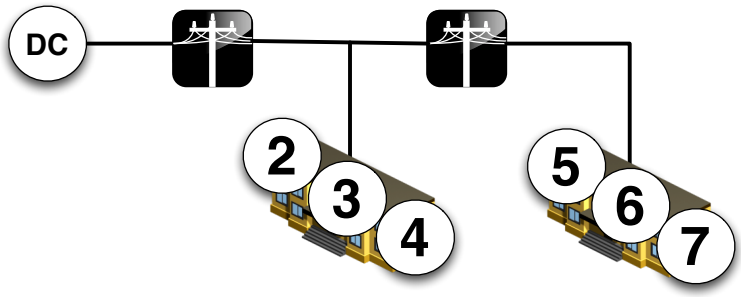
4.4.2 Validation

We validated the simulation tools and models in three topologies (Fig. 4.4), with three different metrics. As these metrics measure the performance of the network in different stages of its life (e.g. initialization, steady state) we performed separate tests for each metric. Table 4.1 presents the number of tests performed per metric per topology.

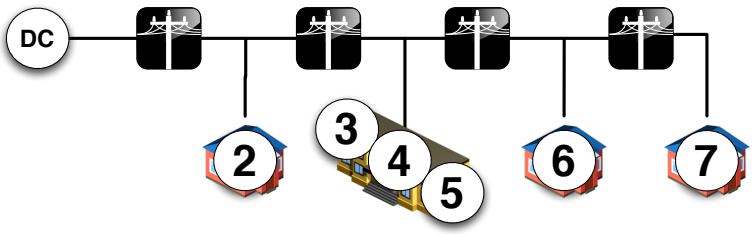
The performance of the network for each metric was collected per SM and averaged over all SM for every scenario. Finally, the simulation results are compared to the experiments performed on the testbed (i.e. the baseline). Results obtained for E2E delay comparison between simulation and implementation in the Rural Case are displayed in Fig. 4.5. While visualization offers a quick way to check the similarity between implementation and simulation, we prefer to use the deviation to formally



(a) Rural topology – low-density area. Meters can communicate directly only with their immediate neighbors.



(b) Urban topology – high-density area. Nodes 2-3-4 can communicate directly with all others, while Nodes 5-6-7 need to go through at least one intermediary to reach the DC.

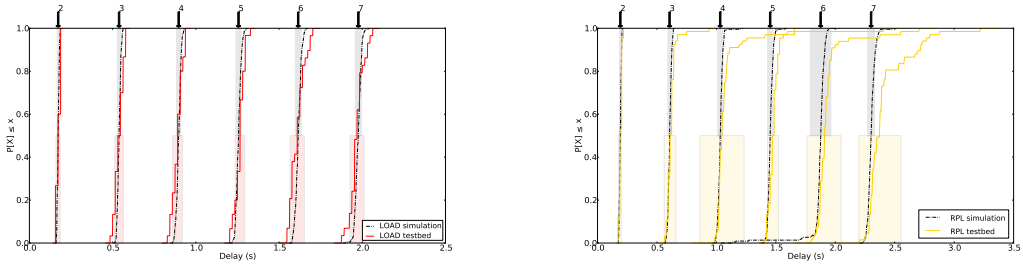


(c) Mixed topology – high- and low- density areas.

Figure 4.4: Topologies used for validation.

	Simulation	DSP
E2E Delay	10 runs of 2h per meter per scenario	2 experiments of 2h per meter per scenario
RF	20 runs per scenario	5 experiments per scenario
RM	20 runs per scenario	5 experiments of 2h per scenario

Table 4.1: Number of tests performed per metric.



(a) LOAD (b) RPL

Figure 4.5: CDF of the E2E delay for a data packet in the Rural Scenario. Rectangles indicate the standard deviation for simulation (top) and testbed (bottom) data. Arrows indicate the node at which the delay was observed.

compare the E2E delay.

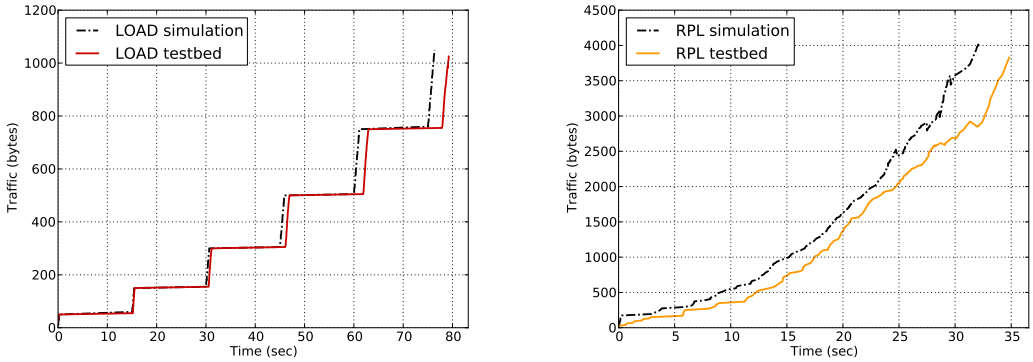
Table 4.2 summarizes the deviation (i.e. the error) under E2E delay metric of the simulation compared to the testbed in percents. E_{avg} is the average error for every given case, e.g. for a given protocol (LOAD or RPL), scenario (Urban, Mixed, Rural) and E2E delay for a given node (nodes 2–7). Similarly, the maximum (E_{max}) and minimum (E_{min}) metrics provide the the worst (resp. best) deviations. The differences simulation/experimentation are limited in most cases (e.g. in all but three cases the $E_{avg} < 6\%$), which validates the behavior of the simulator. The E2E metric is independent from the used routing protocol under a stable topology. Thus, these results validate the simulation of PHY and MAC layers both in terms of model and implementation.

We observe the biggest deviation between the testbed and the simulations for RPL in Mixed and Rural scenarios (Table 6.3). Indeed, Fig. 4.5 reveals a tendency to have more requests with longer E2E delays with every hop in the testbed. The major reason is that RPL was running on a secondary processor (Cortex M3), compared to LOAD, which runs directly on the DSP where we always have consistent behavior simulator/testbed. Indeed, we ported the Contiki implementation of RPL along with the networking stack without optimizing the code for the architecture. Most importantly, the processing of every frame requires Inter-Process Communications (*IPC*) between the DSP and the Cortex M3 for our RPL implementation (and none for the LOAD implementation). All these factors add up to difficult to simulate non-deterministic timing deviations. However, the E2E delays are very close, with most error being inferior to 6%.

We performed validation through several visualization techniques, but in order to have a formal confirmation of the graphical results we calculated the *correlation coefficient* r. We considered the collected data as time series and calculated r over the time. The closer r is to 1, the stronger is the linear relation between the two. The Route Formation (RF) represents a transitional state of the network during

	Node	Difference in % simulation–testbed					
		LOAD			RPL		
		E_{min}	E_{avg}	E_{max}	E_{min}	E_{avg}	E_{max}
Rural	2	0.00	**0.62**	1.22	0.00	**0.48**	1.35
	3	0.04	**1.32**	3.04	0.02	**1.57**	29.91
	4	0.00	**1.32**	3.43	0.05	**5.05**	120.55
	5	0.09	**1.28**	2.99	0.11	**2.70**	14.93
	6	0.00	**2.05**	4.60	0.78	**7.20**	75.41
	7	0.01	**1.82**	5.80	0.04	**10.84**	73.24
Mixed	2	0.01	**0.78**	2.10	0.00	**0.72**	2.12
	3	0.01	**1.82**	39.16	0.00	**2.87**	36.69
	4	0.17	**1.29**	3.56	0.00	**1.03**	7.74
	5	0.02	**1.12**	3.61	0.00	**2.62**	90.70
	6	0.01	**1.39**	32.15	0.00	**1.35**	12.24
	7	0.17	**1.65**	4.99	0.03	**10.49**	177.53
Urban	2	0.01	**0.83**	3.35	0.01	**0.70**	2.16
	3	0.00	**0.78**	2.04	0.01	**1.30**	52.62
	4	0.00	**0.81**	2.27	0.01	**0.65**	2.03
	5	0.05	**1.24**	25.00	0.00	**0.85**	4.83
	6	0.11	**1.29**	4.71	0.01	**0.87**	3.22
	7	0.11	**1.19**	2.90	0.00	**1.29**	14.86

Table 4.2: End-to-End Delay Simulation vs Testbed Error (in %): average (E_{avg}), minimum (E_{min}) and maximum (E_{max}).



(a) LOAD (b) RPL

Figure 4.6: Average traffic generated during route formation for the rural scenario. Individual runs not shown for clarity.

Scenario	RF r	RM r
RPL Rural	0.9951	0.9964
RPL Urban	0.9907	0.9931
RPL Mixed	0.9865	0.9874
LOAD Rural	0.9881	0.9902
LOAD Urban	0.9889	0.9853
LOAD Mixed	0.9877	0.9932

Table 4.3: Route Formation (RF) and Maintenance (RM) correlation – simulation vs testbed.

which the routes are established.

The individual points in Fig. 4.7 present the pairwise correlation between all individual simulations and all experimental runs, with most $r > 0.93$. In contrast, Route Maintenance (RM) corresponds to the steady-state operation of the network. The results for both RF and RM (for averaged time series, as shown in Fig. 7.1) are presented in Table 4.3 and show conclusively the correlation for both RF and RM, with values higher than 0.98 for both LOAD and RPL.

4.5 Conclusion

In this chapter we introduced our IEEE P1901.2 simulator – the physical model, routing protocol implementation, all the way through the simulation scenarios and the approach used for its validation. The simulator was validated against a real-world testbed. The next step is to use the simulation at a larger scale, which would help us highlight problems RPL may encounter with route formation in a more realistic environment, and evaluate the pertinence of the proposed solutions.

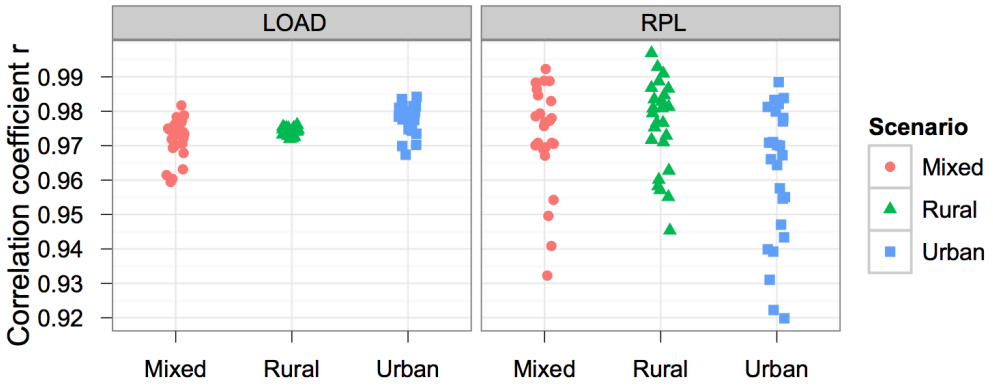


Figure 4.7: Pairwise correlation coefficient r for all simulations vs all experiments for Route Formation.

4

5 Route Formation

As presented in Chapter 3, RPL was not designed having AMI traffic patterns in mind. Indeed, while RPL is optimized for multiple sensors-to-sink traffic, AMI traffic pattern from sink-to-sensors could be critical (meter reading, firmware update, pricing, etc.). In this chapter, we highlight the need of a specific route formation definition for the Smart Grid in Section 5.1 before presenting a weakness in downward route creation that could prevent utilities to communicate with the Smart Meters (Section 5.2). Then, we introduce in Section 5.3 a new way to manage upward routes in order to guarantee efficient downward route creation: *Distributed Dynamic DelayDAO interval adjustment* (4Dia). Section 5.4 presents the evaluation of 4Dia method compared to Contiki. We conclude this chapter with general recommendations for route formation phase in AMI environment in Section 5.5.

5.1 Route Formation

5.1.1 Definition

RPL Route Formation, sometimes referred as convergence time in the literature, is defined as the amount of time needed for all nodes in the network to join the DODAG (e.g. [GKC+12] or [HC11]). As stated in Section 3.3, a node can be considered to have joined the DODAG when it has installed at least one upward route i.e. received at least one DIO. In AMI context, it would mean that the SMs would be able to reach the utilities. However, there is no guarantee that the utilities are able to communicate with the SMs as Route Formation time does not take into account downward routes (installed thanks to DAO messages). Indeed, if the RPL root has not received DAOs from a given SM in the network, they will be unreachable for the utilities. Moreover, in [TdO13], Tripathi *et al.* showed that DAO message emissions' timer can lead to congestion problems in the steady-state phase and prevent RPL from working optimally. Figure 5.1 shows the number of DAO messages that needs to be buffered for a DODAG with a depth of 8, and with 3 children per nodes.

While these results are purely theoretical and do not take into account congestion, they show that the number of messages for lower rank nodes (closer to the root)

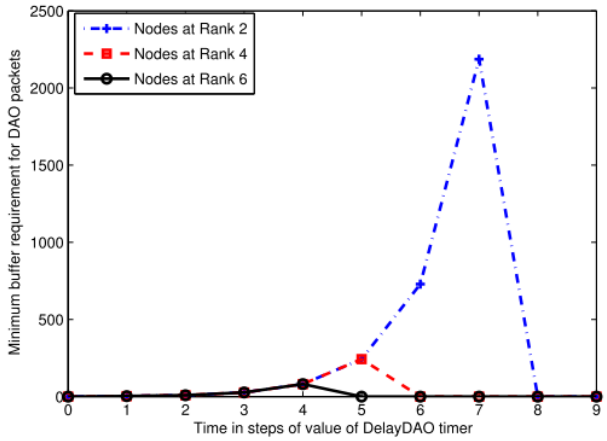


Figure 5.1: Minimum DAO buffer requirements against time for different ranks. (source: Triphati et al. [TdO13])

could lead to cases where nodes are transmitting DAOs at the same time and thus lead to collisions. These collisions prevent the root node to receive DAOs and thus to install downward routes. Therefore, the Route Formation process should not be considered as complete after the upward route installation time but after the time needed for having all downward routes installed on the RPL root in order to be sure to have a complete bidirectional communication between SMs and utilities – Smart Grid's primary enabler.

5.1.2 Route Formation with vanilla Contiki

Our RPL implementation is based on ContikiRPL as we wanted to investigate if some weaknesses attributed to RPL ([HC11, AGBC11b]) are due to a naive/partial implementation of the standard, or if RPL needs to be modified to improve its behavior. We study optimizations in the construction of downward routes and more specifically the influence on *DelayDAO* on it. The *DelayDAO* is the interval used by RPL in order to schedule the sending of a DAO. DAO messages are generated by a node in the following cases:

- One of the parents of the node increments its *DAO Trigger Sequence Number* (DTSN). DTSN is carried by DIO messages and is used by nodes to trigger their sub-DODAG to send DAO messages. Contiki OS always increases DTSN value of the RPL root. This behavior leads to always send DAOs when receiving a DIO from one of its preferred parents;
- Path lifetime should be updated, i.e. the routing table validity lifetime. In Contiki, path lifetime is set to infinite;
- A new node is added in the parent set.

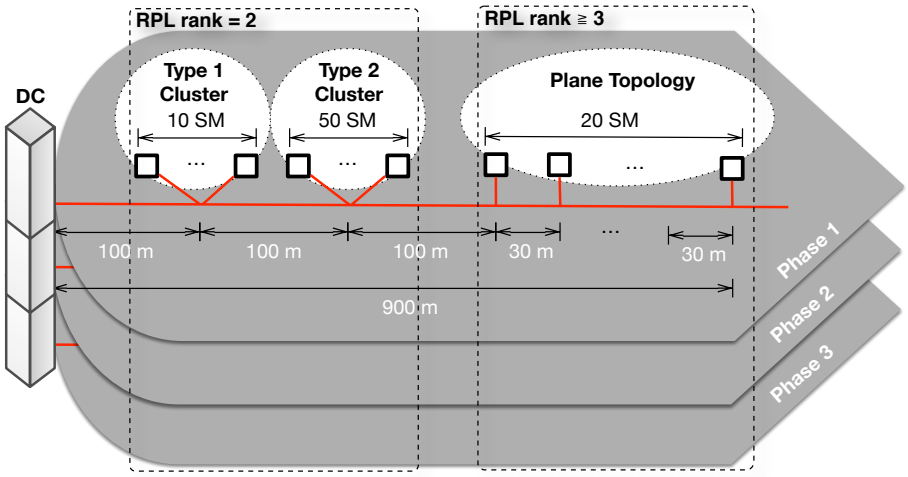


Figure 5.2: Three phase simulation testbed: 240 IEEE P1901.2 nodes and one DC. The layout of all phases is identical.

By default in Contiki, the *DelayDAO* interval is set to be between 4 and 12s. In addition, RPL non-storing mode is not implemented in Contiki, and as such, we were able to evaluate the performance of RPL in storing mode only. However, the problem is identical in non-storing mode as the number of necessary DAO messages remains the same.

5.2 The DelayDAO problem for downward routes creation

5.2.1 Reference scenario

We studied the route formation phase of the network for the reference scenario depicted in Figure 5.2. This scenario represents a typical three-phase AMI deployment where the DC interacts with 240 SMs. Each of the three phases is made of three clusters: Type 1 cluster (10 SMs), Type 2 cluster (50 SMs), and a Plane cluster (20 SMs).

The simulator computes the *Signal Noise Ratio* (SNR) based on the distance between SMs [RLP+] and the decision if two SMs can communicate is based on it. Table 5.1 summarizes the general cluster reachability matrix based on the chosen scenario distances while Figure 5.3 depicts the associated DODAG. The topology we used for our study is typical for a mixed urban-rural SM deployment with Type 1 and Type 2 clusters representing the urban part and Plane Topology representing the rural part. We chose the particular topology parametrization with the primary goal of having an intuitive, easy-to-interpret routing topology. Nevertheless, we performed the same type of analysis under a wide range of randomized topologies

Smart-Meters	Can communicate directly with
Data Concentrator	All phases, Type 1 clusters All phases, Type 2 clusters
Type 1 cluster	Data Concentrator All phases, Type 1 clusters Own phase, Type 2 cluster
Type 2 cluster	Data Concentrator Own phase, Type 1 cluster Own phase, Plane cluster
Plane cluster	Own phase Type 2 cluster

Table 5.1: Communication range for smart meter clusters.

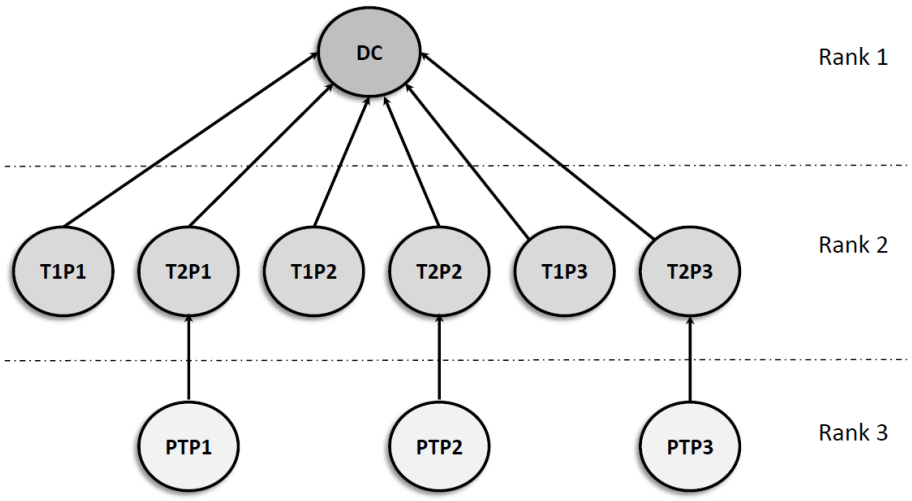


Figure 5.3: DODAG corresponding to the simulated testbed.

and the presented results are representative for the behavior of the protocol.

5.2.2 Route Formation process

The route formation process starts when the DC, which is the RPL root, sends the first DIO message. Upon its reception, the SMs in Type 1 and Type 2 clusters join the DODAG (i.e. constructing upward direct default route to the DC). After joining the DODAG, the SMs in these clusters send their DIO messages based on Trickle algorithm DIO emission. This allows the nodes in the Plane cluster to join the DODAG. This completes the construction of the upward routes.

The construction of the downward routes runs in parallel and is governed by the *DelayDAO* interval. For the first DIO received (or for each DIO received from its preferred parent), a node picks a value in the *DelayDAO* interval. Once this value elapses, the DAO is sent. After receiving DIO from the DC, the nodes in Type 1 and Type 2 clusters are going to send their DAOs after a duration in *DelayDAO* interval. In turn the nodes in the Plane cluster are going to send their DAO messages towards the DC after a duration in *DelayDAO* interval once DIO from Type 2 clusters are received. The route formation process is considered complete when the DC has downward routes to all SMs in the network.

5.2.3 Performance degradation and hidden nodes

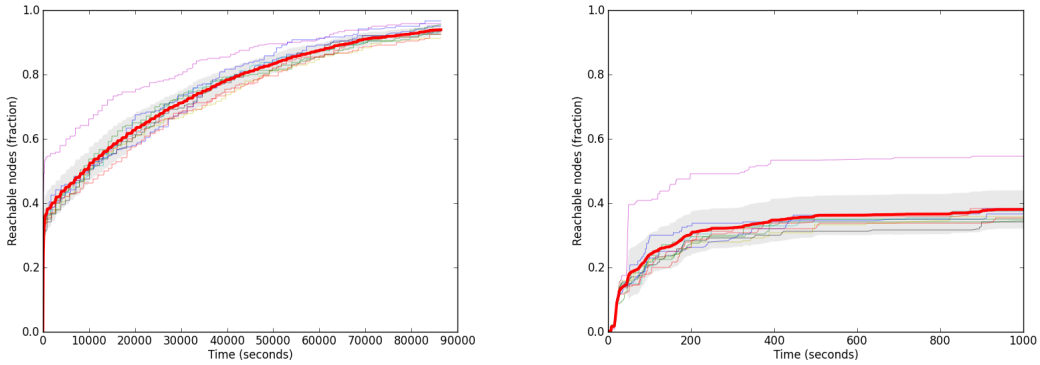
Parameter	Value
Number Of Nodes	240
Trickle	Min Interval [2;4s] - Max Interval [524;1048s]
DelayDAO	[4;12s]
OF	OF0
Metric	Hop-Count

Table 5.2: Simulation parameters.

We performed 10 runs of 24 hours simulated time with the parameters given in Table 5.2 to observe the percentage of downward routes known by the DC. Please not that Trickle min and max values stands respectively for minimum/maximum DIO interval emission. The results (see Table 5.3) show that it may take more than $24h$ to discover 95% of the smart meters. Only 4 of the 10 runs discovered 95% of the SMs, and none of the runs reached a full network discovery. In the majority of the cases, a utility which deploys RPL with default Contiki OF0 behavior will not be able to reach 5% of the smart meters after 24h. Fig 5.4 shows the evolution over time of the route discovery.

Known downward routes (%)		10%	25%	50%	75%	95%	100%
Contiki Default		23.9 ± 3.3	138.7 ± 31.3	8972.6 ± 2378.1	34810.5 ± 4493.7	79064.9 ± 9794.6	n/a
DelayDAO	U=24	17.8 ± 0.5	25.1 ± 1.8	72.2 ± 13.5	134.3 ± 16.6	545.1 ± 156.6	3189.4 ± 1064.2
	U=36	18.2 ± 0.6	28.3 ± 4.9	62.0 ± 15.5	124.4 ± 13.5	260.9 ± 43.5	770.0 ± 212.7
	U=48	18.9 ± 1.0	28.4 ± 3.7	50.9 ± 1.9	99.3 ± 10.5	214.3 ± 26.5	862.7 ± 632.5
	U=60	20.1 ± 1.3	35.7 ± 4.9	54.2 ± 1.2	101.3 ± 11.9	253.4 ± 54.6	657.6 ± 181.7
	U=72	20.6 ± 1.2	39.8 ± 2.5	55.8 ± 1.7	93.7 ± 5.5	239.0 ± 46.5	591.3 ± 232.7
	U=84	21.8 ± 1.3	39.8 ± 3.9	58.5 ± 1.7	98.1 ± 2.2	255.1 ± 53.0	824.3 ± 253.1
	U=96	23.9 ± 2.5	44.8 ± 2.0	63.8 ± 3.6	101.4 ± 3.3	222.0 ± 56.1	657.9 ± 249.8
	U=108	25.1 ± 4.1	45.8 ± 5.0	68.2 ± 9.2	101.8 ± 4.1	219.7 ± 45.2	721.6 ± 342.1
OM-4Dia	K=1.2	24.0 ± 1.3	75.9 ± 16.8	192.6 ± 37.5	384.3 ± 75.2	1188.9 ± 337.8	3049.7 ± 620.0
	K=1.5	24.0 ± 1.3	64.5 ± 18.0	106.8 ± 16.7	161.4 ± 32.7	300.6 ± 48.8	879.7 ± 187.1
	K=2	24.0 ± 1.3	49.7 ± 8.3	87.1 ± 19.2	136.0 ± 9.9	292.2 ± 34.4	614.1 ± 115.5
	K=3	24.0 ± 1.3	49.7 ± 6.4	71.6 ± 15.0	141.7 ± 15.5	247.1 ± 40.4	683.2 ± 212.6
	K=4	24.0 ± 1.3	51.0 ± 6.7	72.5 ± 10.8	123.6 ± 17.6	267.0 ± 40.2	673.4 ± 220.1
P-4Dia	D=1.2	25.2 ± 3.4	46.2 ± 3.2	69.4 ± 7.3	103.6 ± 3.0	229.8 ± 48.0	838.2 ± 299.6
	D=1.5	25.3 ± 3.4	46.3 ± 2.9	68.0 ± 6.4	103.8 ± 2.6	192.2 ± 37.9	651.4 ± 267.5
	D=2	25.5 ± 3.4	46.5 ± 3.0	70.0 ± 8.3	104.4 ± 4.3	230.8 ± 39.1	763.8 ± 260.1
	D=3	26.0 ± 4.1	46.4 ± 3.1	70.3 ± 7.5	104.2 ± 4.2	207.3 ± 30.2	5997.3 ± 11777.0
	D=4	25.6 ± 3.7	46.0 ± 3.1	71.4 ± 8.6	103.5 ± 3.4	212.5 ± 43.7	9654.2 ± 11595.2
OA-4Dia		24.0 ± 1.3	50.1 ± 8.6	90.9 ± 20.5	143.2 ± 14.9	265.6 ± 42.7	532.3 ± 118.8

Table 5.3: Average time in seconds (± confidence intervals at the 95% level) to discover a given percentage of downward routes by the RPL root for different strategies. Results of 10 independent runs. The blue values indicate the best strategies, while red values point simulations which did not reach the given percentage in 24h. No runs reached 100% with Contiki.



(a) Contiki Default in 24h.

(b) Contiki Default (zoom into first 1000s).

Figure 5.4: Route Formation Process for Contiki Default values.

In IEEE P1901.2, unicast messages (such as DAO) are retransmitted if no acknowledgment is received until a threshold which is set to 5 by default. If it is reached, the frame is dropped. We monitored the RPL rank of SMs whose DAO messages are dropped due to this threshold. The results show that in 99% of the cases these SM have RPL rank of 2 (Type 1 and Type 2 clusters).

In IEEE P1901.2 frame transmission is governed by CSMA/CA. Before transmitting, a node waits for a random backoff timer and then checks the channel availability. In our scenario, Type 2 clusters are unable to communicate directly with other Type 2 clusters belonging to a different phase because of signal attenuation, and all communications with SM between them are heavily penalized. Thus, each DAO transmitted by a node belonging to Type 2 clusters is potentially going to prevent CSMA/CA from other Type 2 cluster to work correctly (as well as DAO sent by plane topology SMs as they are forwarded by Type 2 cluster nodes). This is the source of the classical problem of a the hidden node, which has been described for PLC in [HAN]. A simple analytical calculation confirms the results obtained. Knowing that there is potentially 70 hidden nodes on each phase (50 Type 2 cluster nodes + 20 Plane Topology cluster nodes), 210 SMs will have to flow out their own DAO in 8 seconds (i.e. *DelayDAO* interval length) which gives approximatively 38ms per DAO. Being unicast frame, DAO needs to be acknowledged so channel occupancy of a DAO can be obtained thanks to Equation 5.1:

$$DAO_{channel\_occupancy} = T_{DAO} + T_{Ack} = 125 + 15 = 140ms \tag{5.1}$$

The *DelayDAO* interval is too short compared to the channel occupation time of a DAO.

5.2.4 Parameter exploration

In order to see how the *DelayDAO* interval value is influencing the route formation process, we tested the same scenario with eight different *DelayDAO* intervals – $[4s; Us]$, where $U \in \{24, 36, ..., 96, 108\}$. The results provided in Table 5.3 show the influence of the choice of the *DelayDAO* interval on the route formation process. The route formation time varies significantly. For a *DelayDAO* upper bound greater than 36s, 100% of the downward routes are known in less than one hour. For the cases of 60s and 72s, the convergence time for 100% of the network is less than 15 minutes. However, the performance improvement is not inversely proportional to the upper interval bound – having a bigger *DelayDAO* interval does not guarantee better performance. This observation confirms the importance of having a dynamic *DelayDAO* interval during route formation phase. In case of using a static *DelayDAO* interval, if not correctly parametrized, the utility operator may be unable to communicate with some of SMs in the network.

5.3 THE NEED FOR A DYNAMIC DELAYDAO PER NODE

We propose the *Distributed Dynamic DelayDAO interval adjustment* (4Dia) solution to overcome Route Formation problems raised in Section 5.2.3. We assume that a node has no global knowledge of the total number of nodes in the network, the number of direct neighbors, nor the position of a node in the network (e.g. its rank). Instead of using these data which can be obtained during the steady-state of the network but not during the route formation, we propose to base the *DelayDAO* interval computation on the delivery rate of DAO messages. A failed DAO transmission is considered as a signal that there are too many collisions and the node should limit the rate at which it is sending its DAOs.

The DAO-ACK mechanism could be used to confirm the successful transmission of a DAO message. However, we do not want to add new message exchanges during the route formation period, as each such message increases the collision probability. Moreover, as IEEE P1901.2 includes frame acknowledgments, the addition of an explicit DAO-ACK message actually adds two frames to be exchanged (DAO-ACK-frame and DAO-ACK-ack frame). Instead of adding new explicit messages, we can assume that upon an IEEE P1901.2 acknowledgment of the DAO frame, the DAO message was successfully received by the destination. This cross-layer approach allows the dynamic adaptation of the DelayDAO timer without adding any additional traffic to the network in the case of an IEEE P1901.2.

In this chapter, we investigate thee strategies for 4Dia – optimistic-multiplicative, optimistic-additive and pessimistic divisive. In the optimistic strategies we start with a small initial interval which is increased upon DAO message loss. The pessimistic one starts with a large initial interval, which is decreased upon DAO message

acknowledgment.

5.3.1 Optimistic-multiplicative 4Dia (OM-4Dia)

This adaptation defines the DelayDAO interval as $[4s; K^i 12s]$, where K is a multiplicative factor, and i is the number of DAO message reemissions (e.g. $i = 0$ on the first DAO message). A higher extreme bound *EXTREME_BOUND* is also defined for *DelayDAO* upper bound (*delayDAOmax*). It allows to avoid too large *DelayDAO* in case of many successive DAO reemissions. The adaptation algorithm is shown in Algorithm 8, along with interaction between RPL and the PHY/MAC layers:

Algorithm 8: 4Dia – CORRECTION_FACTOR and OPERATOR corresponds respectively to "K" and "<" for OM-4DIA and "1/D" and ">" for P-4Dia

```
DAO_Send:
DelayDAOtime := Random(DelayDAOmin, DelayDAOmax)
Sleep(DelayDAOtime)

Mac_Send:
Result := MacLayer.SendFrame(DAOmessage)
if (Result = Mac_ACK) then
  Goto End
end if
if (MacRetransmissions < MacMaxRetransmissions) then
  MacRetransmissions += 1
  DelayDAOmax := CORRECTION_FACTOR * DelayDAOmax
  if (DelayDAOmax OPERATOR EXTREME_BOUND) then
    DelayDAOmax := EXTREME_BOUND
    Goto DAO_Send
  end if
end if
```

5.3.2 Optimistic-additive 4Dia (OA-4Dia)

In this strategy, upon reaching the maximal number of retransmissions, instead of multiplying the DelayDAOmax by a given factor, it is increased by a constant. The constant is the initial DelayDAOmax as to provide for a less aggressive reaction to the network conditions, while still providing a dynamic adjustment to high density of hidden nodes. Thus, if the initial DelayDAOmax is 12s, the consequent values will be 24s, 36s, 48s, etc. As with OM-4Dia, an upper bound should be fixed (9× DelayDAOmax by default).

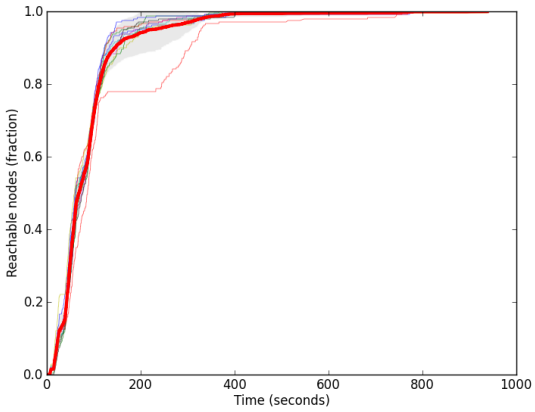


Figure 5.5: P-4Dia (D=1.5) in 1000s.

Figure 5.6: Fraction of known smart meters during the Route Formation phase. The red line indicates the mean value for the 10 individual runs (which are shown as light colored curves). The gray region indicates the standard deviation around the mean.

5

5.3.3 Pessimistic 4Dia (P-4Dia)

In the optimistic approach, we multiply DelayDAOmax in case of DAO transmission failure. This approach considers that few problems will occur. We defined a pessimistic approach by choosing a large initial value for the DelayDAO interval (i.e. *DelayDAOMax*). Reacting to favorable network conditions, we apply a reduction factor – D – to avoid being overly pessimistic and have long route discovery delays. To avoid too short DelayDAO interval in case of successive DAO reemissions, a lower extreme bound *EXTREME_BOUND* is used. Algorithm 8 outlines the modified algorithm.

5.4 Results

For each of the proposed strategies we performed 10 independent simulation runs. Table 5.3 summarizes the times necessary to reach a given percentage of discovered SM. We calculated the confidence intervals at the 95% level using Student's t-distribution, also provided in the table. As the default Contiki values, we used the scenario shown in Figure 5.2. All strategies provide significant performance improvements over the Contiki RPL.

5.4.1 Optimistic 4Dia algorithms

For OM-4Dia we evaluated the behavior under five values for K – 1.2, 1.5, 2, 3, and 4, with initial values for the DelayDAO interval taken from Contiki (i.e. *DelayDAOmin*=4s and *DelayDAOmax*=12s). From Table 5.3 we can see that the RPL root discovers all downward routes in less than 1 hour independently of K. The worst performance is observed when $K = 1.2$, with all other values completing in less than 17 minutes. For values bigger than 1.5 the differences become statistically insignificant. Independently of the value of K, the optimistic adaptive strategy outperforms significantly the statically allocated, classical DelayDAO interval which proves the need of an adaptive strategy for DelayDAO timer.

We evaluated OA-4Dia with the same initial default parameters as Contiki. From Table 5.3 it can be seen that this algorithm is an overall good choice when compared to OM-4Dia and to P-4Dia, and the fact that it does not require additional parametrization can be considered an advantage.

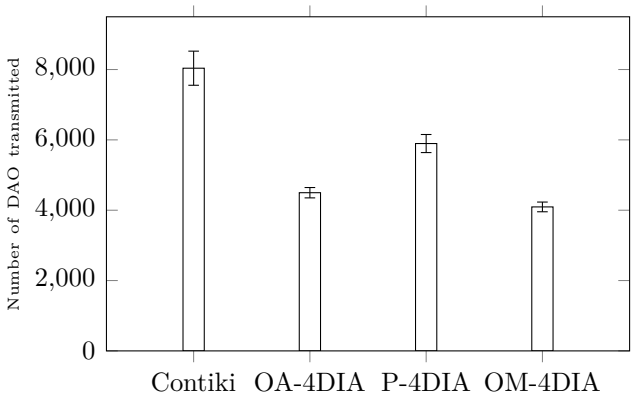
5.4.2 Pessimistic 4Dia

We used several values for the evaluation of the P-4Dia strategy – $D \in 1.2, 1.5, 2, 3$. Figure 5.5 illustrates the fraction of discovered smart meters over time for $D = 1.5$, with all details given in Table 5.3. DelayDAOmax is initialized to 108s while DelayDAOmin is 4s. P-4Dia is more sensitive to the choice of its parameter D than OM-4Dia. Indeed, with the increase of D, the performance deteriorates, with great variability among the individual runs. Values bigger than 2 should be avoided, as they lead to instability in the route formation process – and the only case of the proposed strategies where one of the simulations did not finish the route formation process in the allotted 24h.

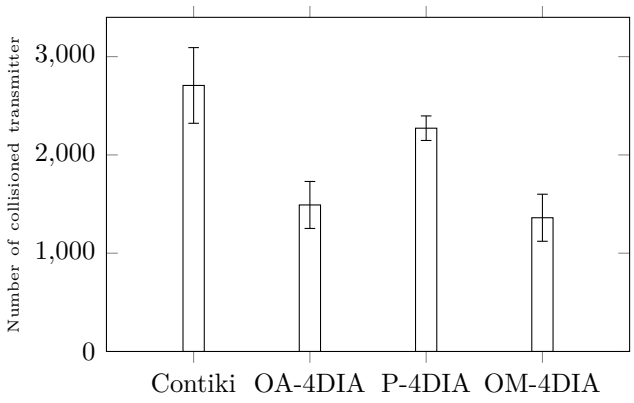
5.4.3 Results interpretations

In order to analyze the results obtained, we decided to monitor route formation process during one hour of simulated time for Contiki, OA-4Dia, P-4Dia and OM-4Dia. We studied total number of DAO messages transmitted in the network, number of transmitting nodes in collision, and number of DAO messages dropped due to maximum number of retransmission.

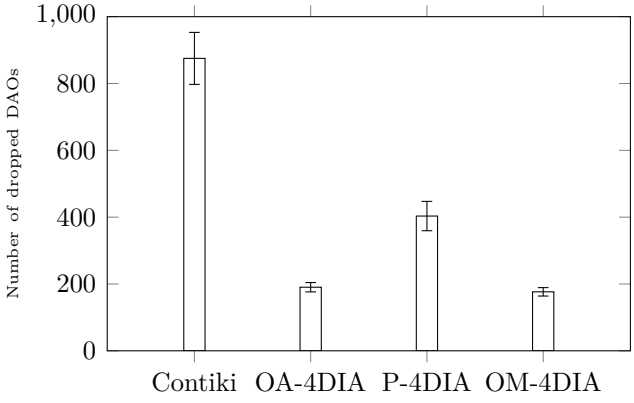
Figure 5.7(a) demonstrates that even if Contiki transmits the highest number of DAO on the network, it does not lead to better performances. On the contrary, it leads to a dramatic increase in the amount of transmitter in collision as shown on Figure 5.7(b). It has the consequence to result in a huge number of DAO messages dropped as depicted on Figure 5.7(c) and then to prevent an optimal route formation.



(a) Number of transmitted DAO for one hour of simulated time depending on the strategies used.



(b) Number of collisioned transmitter for one hour of simulated time depending on the strategies used.



(c) Number of DAO dropped for one hour of simulated time depending on the strategies used.

Figure 5.7: Comparison of Route Formation process.

5.5 Discussion and recommendations

The default Contiki DelayDAO values may be unsuitable for AMI PLC deployments. A utility deploying a network with this parametrization may have to wait more than 24h before being able to reach all SMs. Choosing static values can significantly improve the performance, but the choice is not straightforward for optimal behavior of the network. Having an adaptive decentralized algorithm can provide better performance, but should also be configured appropriately.

For an SM network with similar topology, use a fixed upper limit of $60s$, P-4Dia with $D = 1.5$, or OM-4Dia with $K = 3$. An overall good candidate which does not require parametrization is to use OA-4Dia, which is also recommended as a suitable candidate for a generic topology.

To the best of our knowledge, [GKC+12] is the only paper written on RPL route formation. In this paper, the author express convergence time as "the time at which the DAG is completely constructed and all nodes in the network have joined DAG". With such a definition for convergence time, only upward routes installation are taken into account. We showed that downward routes installation is a critical step that could lead to a significant number of SMs to be unreachable for the utilities. In [TdO13] Tripathi *et al.* studied congestion problems that occur when DelayDAO timer is not appropriately chosen. Although the paper focuses on radio communications it is similar. The authors proposed several solutions both for storing and non-storing mode. The main idea is to have enough time to transmit all DAOs in the network. The authors proposed centralized and distributed approaches. The distributed solution is not suitable for storing mode as it relies on end-to-end DAO-ACK from SM to RPL root and in storing mode, the DAOs are acknowledged at every single hop.

For the centralized approach, the first proposal is that the RPL root is computing and distributing the DelayDAO interval dynamically depending on the rank and the number of nodes at a given rank. The deeper a node is situated in the DODAG, the bigger the DelayDAO interval is, with a correction factor applied depending on number of nodes at a given rank. The second possibility is to use DAO aggregation and to set the DelayDAO timer inversely proportional to the rank. Nodes closer to the RPL root wait longer in order to aggregate as much DAO messages from their child nodes as possible. Nodes farther away from the RPL root wait less, as they are expected to have less DAO messages to aggregate.

Both solutions require a global knowledge of the network as they are based on the rank of the node and are applicable for the steady-state regime of the network only. During the route formation the information required by these algorithms is not available. As we showed previously, the number of known routes can be incomplete even after a long period.

Thus, as stated in [TdO13], the DelayDAO interval should be dynamically adapted.

However, contrary to their centralized approach where DelayDAO interval is set for a given rank, during the route formation it should be computed individually for each node, independently from its rank.

IETF RPL provides all mechanisms to enable future proof, robust and scalable networks in lossy environment. We presented in this chapter an analysis of the Contiki RPL stack, which confirmed the observations that parameter selection has to be set carefully depending on the type of targeted application. We proposed three dynamic adaptation mechanisms which improve the performance of the routing algorithm during the route formation phase. These mechanisms refine the behavior of RPL in a standard-compliant way and are relevant to narrowband PLC networks, as well as topologically similar wireless networks, e.g. IEEE 802.15.4 multi-hop AMI networks. In addition, we proposed an independent, IEEE P1901.2/RPL specific cross-layer optimization for the downward route construction messages.

5.6 Conclusion

5

In this chapter, we highlighted the need for a novel definition for convergence time in the context of Smart Grid as well as the DAO messages congestion problem. We proposed the new 4Dia solution that allows to speed-up route formation. In the next chapter, we are going to put the emphasis on the need of a new mechanism to handle link-breakage management in the SG.

6

Route Maintenance

RPL has been studied both in the cases of global and local repair. As described in Section 3.3, global repair occurs when the routes need to be refreshed (e.g. re-created) over the entire DODAG while local repair happens in case a node loses all of its parents. These two processes are important for RPL as they allow to react to network failure. However, both global repair and local repair occur in "extreme" situations:

- Global repair is triggered when the RPL root increments the *DODAGVersionNumber*. This operation is administratively performed or can be triggered depending on time. This operation should be performed only if all routes need to be reconstructed i.e. a major power outage or unacceptable network performance;
- Local repair is triggered when a node is unable to select a parent in its parent set i.e. no parent is offering an acceptable performance.

In this chapter, we are going to highlight the fact that link-failure detection is as important as global and local repair. Indeed, due to AMI's traffic patterns, parent's failure detection could take a huge amount of time. In order to overcome that problem, we propose a new mechanism: *Fast and Reactive Link-failure Detection* (FRLD). It uses two new methods; one for Fast link-failure detection of Preferred Parent: *Neighbor Unreachability Detection for Preferred Parent* (NUD-PP) and the other one for Fast link-failure reaction: *Aggressive Downward Route Management* (ADRM). The former accelerates the parent failure detection while the latter helps to reinstall faster downward routes in order to shorten link breakage between the RPL-root and the Smart Meters.

Section 6.1 presents in detail the *Expected Transmission Count* (ETX) metric with *Minimum Rank with Hysteresis Objective Function* (MRHOF) as *Objective Function* (OF). Section 6.2 highlights the link detection problem while Section 6.3 describes the proposed solution. Section 6.4 concludes this chapter by analyzing past works done on the topic.

6.1 THE ETX METRIC

De Couto et. al introduced the *Expected Transmission Count* (ETX) metric in [DCABM03]. ETX metric aims to minimizes the expected total number of packet transmissions (including retransmissions) needed to successfully deliver a packet to the destination. ETX is computed from Equation 6.1.

$$ETX = \frac{1}{d_f * d_r} \tag{6.1}$$

where d_f is the the forward delivery ratio i.e. the probability that a data packet successfully arrives at the destination and d_r is the the reverse delivery ratio i.e. the probability that the acknowledgment packet is successfully received. Thanks to d_r and d_f, the ETX metric takes into account the effects of link loss ratios and asymmetry.

The ETX metric for a given RPL node is the sum of the ETX from the node to the RPL root when used conjointly with MRHOF OF. Thus, ETX can be computed from Equation 6.3.

$$ETX = ETX_{path} + ETX_{link} \tag{6.2}$$

where:

- ETX_{path} is the ETX from the node's preferred parent to the RPL root
- ETX_{link} is the ETX of the link to the node's preferred parent

ETX_{path} is transmitted via the rank of the preferred parent while the node can estimate the ETX_{link}. In Contiki, ETX for a link with a given parent is implemented as an *Exponentially Weighted Moving Average* (EWMA) filter as given in Equation 6.3.

$$ETX_{link} = ETX_r * \alpha + ETX_p * (1 - \alpha) \tag{6.3}$$

where:

- α, a time-weight coefficient, is set to 0.9 by default
- ETX_r is the previously recorded ETX i.e. the ETX_{link} before the arrival of a new ETX measurement ETX_p
- ETX_p is the ETX for the current packet transmission

ETX_p is computed with Algorithm 9. with MAX_ETX set to 10 and *numtx* equals to the number of transmissions needed to receive an acknowledgment. The usage of an EWMA filter is a conservative approach. Indeed, a value of 0.9 for α means that previously recorded ETX_r are much more important than the new measured ETX_p. Moreover, ETX is estimated only for the link currently being used, i.e. the preferred parent, as no traffic is sent on other links. For other candidate

Algorithm 9: ETX computation for a given packet transmission

```
if (TX_SUCCEED) then
    ETX_p = numtx
else
    ETX_p = MAX_ETX
end if
```

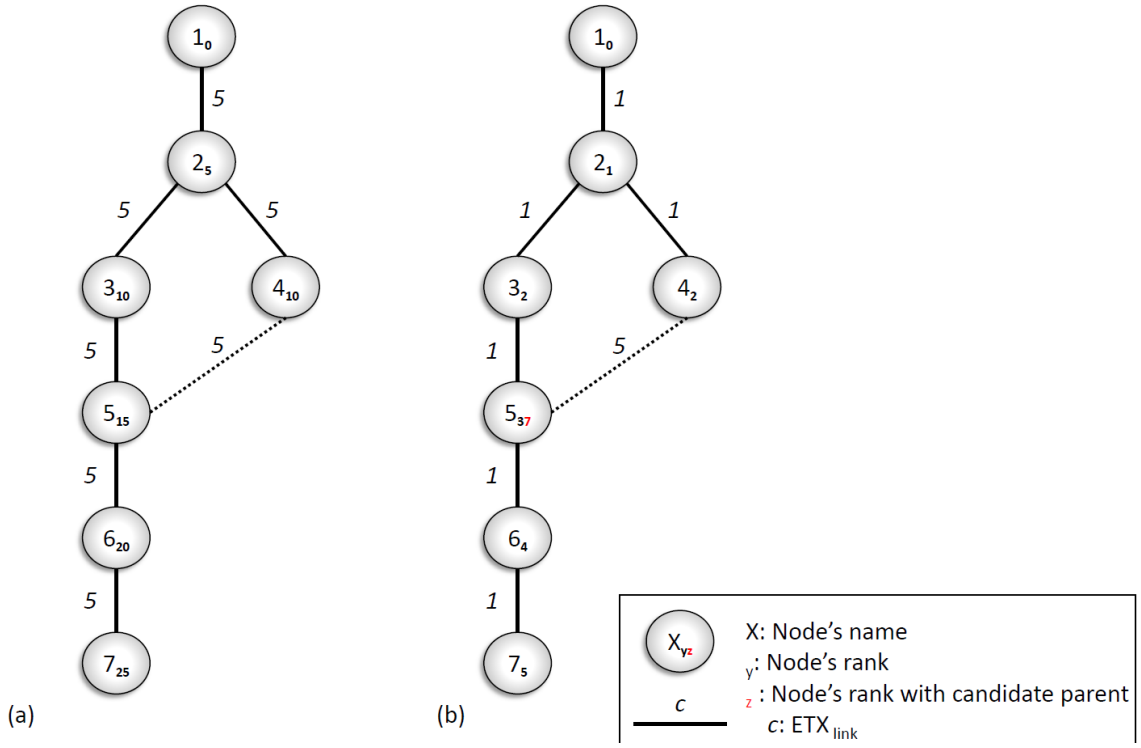


Figure 6.1: DODAG topology and associated rank at startup (a) and in steady-state phase(b).

parents, and when the ETX_{link} is not yet estimated (i.e. when a potential parent is detected), ETX_{link} is initialized to ETX_{init} which has a default value of 5 in Contiki.

6.2 THE LINK-FAILURE DETECTION

We consider the scenario depicted in Figure 6.1.a (The figure represents the DODAG of the topology) with parameters indicated in Table 6.1. Node 1 acts as a border router. Each node is directly connected to one preferred parent except node 5 that has node 3 as a preferred parent and node 4 in its candidate parent set. As described in Section 6.1, during the initialization phase (Figure 6.1.a), ETX_{link} is initialized to ETX_{init} (5). Thus, each node is having a rank equal to its preferred

Parameter	Value
Number Of Nodes	7
Trickle	Minimum Interval [2;4s] - Max Interval [524;1048s]
DelayDAO	[4;12s]
OF	MRHOF
Metric	ETX

Table 6.1: Simulation parameters.

parent with ETX_{init} added. If we consider now the steady-state (Figure 6.1.b), the ETX_{link} is going to decrease until ETX_{min} i.e. 1 except for the link between node 5 and node 4 (as ETX is evaluated only with preferred parent). EWMA can be assimilated to a sequence which has the properties of Equation 6.4. From this, we can compute the number of messages needed for node 5 to switch from parent 3 to parent 4 in case of link-failure between node 5 and 3. Note that in case of failed transmission, ETX_P is increased from 10.

$$\begin{aligned} ETX_{link(N+1)} &= ETX_{link(N)} * \alpha + ETX_p * (1 - \alpha) \\ &= ETX_{link(N)} * 0.9 + 1 \end{aligned} \tag{6.4}$$

We are using MRHOF OF so Node 3 is going to switch to Node 4 if algorithm 9 is verified.

Algorithm 10: MRHOF Hysteresis function

$P3$ is the current best parent - $P4$ is a candidate parent
if $P3_{path\ cost} + PARENT\_SWITCH\_THRESHOLD > P4_{path\ cost}$ **then**
  Switch to $P4$ as a preferred parent
end if

$PARENT\_SWITCH\_TRESHOLD$ is set to 0.5 in Contiki and $path\_cost$ is the sum of the preferred parent rank and ETX_{link}. Node 3 and Node 4 having the same rank, the switch is going to occur when ETX_{link} of Node 3 and Node 4 are going to differ of 0.5. Table 6.2 provides the calculation of the first 8th occurence of the sequence 6.4. We can see that 8 failed transmission are needed in order to trigger the parent switch.

Now, let's consider the case where node 1 is sending to node 7 (i.e. downward traffic from border router to node) every 10 seconds. After S_{Off} (see Table 6.3), Node 3 is switched-off to emulate node's failure and link breakdown. We then observe the end-to-end (E2E) delay at node 7 in order to see how long it takes for node 5 to detect link breakdown and to switch to node 4 as its preferred parent (i.e. time T_{resume} needed to resume communication between Node 1 and 7).

ETX_{link3}	ETX_{link4} - ETX_{link3}
1	-4
1,9	-3,1
2,71	-2,29
3,43	-1,56
4,09	-0,90
4,68	-0,31
5,21	0,21
5,69	0,69

Table 6.2: Number of failed messages needed in order to produce a sufficient ETX_{link} increase in order for Node 5 to switch from Node 3 to Node 4 as a preferred parent. Node 5 being unevaluated, its ETX_{link} remains constant to 5.

	$T_{resume}(second)$		
$S_{Off}(second)$	**Contiki Default**	**FRLD**	
		$T_{NUD-PP} = 30s$	$T_{NUD-PP} = 240s$
3000	$270,5s \pm 51,1$	$36,6 \pm 3,8$	$182,9 \pm 69,9$
3600	$563,9 \pm 151,4$	$19,91 \pm 1,9$	$152,81 \pm 27,1$
4000	$604,5 \pm 42,4$	$29,6 \pm 3,8$	$205,1 \pm 30,5$

Table 6.3: Average time in seconds ($T_{resume} \pm$ confidence intervals at the 95% level) to resume communication with different node switching-off time (S_{Off}). T_{NUD-PP} indicates the emission timer for NUD-PP. Results of 30 independent simulation runs.

Table 6.3 shows results obtained for three different values of Switching-off time for Node 3 with Contiki's default behavior. We can notice that time for resuming the communication varies from 270s (4 minutes) to more than 604s (10 minutes) depending on S_{Off}. This delay represents the amount of time needed by the network to detect and react to the link failure.

Resuming communication is made of two main phases: *detection* and *reaction*. Figure 6.2.b represents the first step, i.e. the detection of the link breakdown. As the data traffic pattern is downward, no upward data traffic is generated. The only unicast packets sent upward are DAO messages. As detailed in Section 3.3, DAO are emitted if a DIO with increased DTSN is received, a new node is added as a parent, or path lifetime should be updated. Path lifetime is set to infinity in Contiki, and our topology is static so no new parent is going to be added for node 5. Thus, the only way to send a DAO in the topology is to receive a DIO with an increased DTSN which is the default behavior of Contiki RPL. DIO emission is governed by Trickle timer, which can vary from several minutes to an hour (1048 seconds at maximum in Contiki) if the conditions are stable. Since after less than one hour DIO emission interval is between 524 and 1048 seconds, we decided to test three different values

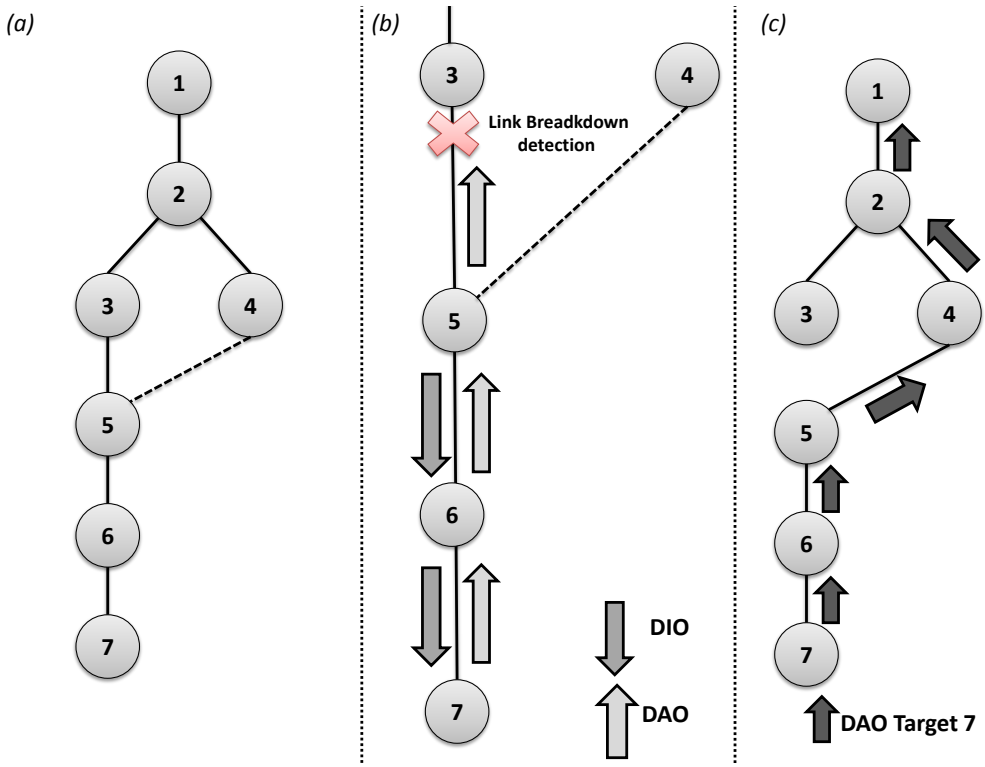


Figure 6.2: DODAG topology and needed step for resuming communication in case of a failure of Node 3.

of S_{Off}. In the worst case, a DIO is going to be transmitted only after 1048s. The nodes that receive the DIO are going to schedule a DAO so whichever is the DIO receiving node, Node 5 is going to send its own DAO or forward a DAO to Node 3. As Node 3 is switched-off, the DAO sent by Node 5 is going to increase ETX as no acknowledgment will be received. Once the ETX reaches the hysteresis threshold, Node 3 is going to switch to Node 4 as a preferred parent. However, there still remains the reaction part.

Indeed, Node 1 and more particularly Node 2 are still having the former route to Node 3 in order to reach Node 7. Thus, the last step is that the DAO coming from Node 7 arrives to Node 1 in order for it to install the corresponding route to Node 7. Only once detection plus reaction are achieved, the downward traffic from Node 1 to Node 7 will resume.

6.3 Fast link-failure detection for Preferred Parent

Our solution is using a slightly modified version of *Neighbor Unreachability Detection* (NUD) that is presented in the next section.

6.3.1 Neighbor Unreachability Detection

The NUD mechanism allows to detect the reachability of other nodes in the network and can be used to unveil link breakdown. As Contiki comprises a full IPv6 stack, it implements Neighbor Unreachability Detection (NUD). NUD works with different states to know neighbor reachability:

- INCOMPLETE: Address resolution is in progress and the link-layer address of the neighbor has not yet been determined;
- REACHABLE: the neighbor is known to have been reachable recently (within tens of seconds ago i.e. REACHABLE_TIME);
- STALE: The neighbor is no longer known to be reachable but until traffic is sent to the neighbor, no attempt should be made to verify its reachability;
- DELAY: The neighbor is no longer known to be reachable, and traffic has recently been sent to the neighbor. Rather than probe the neighbor immediately, however, delay sending probes for a short while in order to give upper-layer protocols a chance to provide reachability confirmation;
- PROBE: The neighbor is no longer known to be reachable, and unicast Neighbor Solicitation (NS) probes are being sent to verify reachability.

Neighbor Solicitation (NS) is the message that explicitly asks a node to reply with a neighbor advertisement and then to check node's reachability.

6.3.2 Fast link-failure detection for Preferred Parent:NUD-PP

Once in STALE mode for a neighbor, if no data is sent to the corresponding neighbor, no verification is done for neighbor reachability. We highlighted that phenomena in part 6.3.1. To optimize link-failure detection, and more precisely the link to the preferred parent, we introduced a new behavior for neighbor cache entry for the preferred parent. The principle is that preferred parent neighbor cache entry is going directly from REACHABLE to PROBE state. This strategy is called Neighbor Unreachability Detection for Preferred Parent (NUD-PP). Thus, if no data traffic is sent, reachability of preferred parent is always going to be checked in a timescale of tens seconds (i.e. REACHABLE_TIME in NUD standard) by sending a neighbor solicitation. However, in order to operate minimum changing for NUD protocol, we replace the REACHABLE_TIME of the preferred parent by a new timer called T_{NUD-PP}. The detection of dead parent is then going to be shortened at the price of higher signaling trafic overhead (depending on T_{NUD-PP}). It is important to note that this slight modification of Neighbor Discovery remains interoperable with ND standard.

6.3.3 Fast link-failure reaction: Aggressive Downward Route Management (ADRM)

As depicted in Figure 6.2, resuming communication between Node 1 and Node 7 does not only depend on detecting preferred parent's link failure. Node 1 should also have the route to Node 7 (i.e. Node 2 must change it's downward route). This event can be quite long as DAO sending for Node 7 depends on receiving a DIO from its preferred parent 6. In order to optimize downward route installation, we propose a new Aggressive Downward Route Management (ADRM). In case of preferred parent change, all downward routes managed by the node which changes its preferred parent lead to a DAO emission with the corresponding target (Node 5, 6 and 7 in our case in order to node 1 to have the new downward routes). Thus, downward routes installation time is going to be significantly decreased.

Combining both NUD-PP and ADRM leads to our Fast and Reactive Link-failure Detection (FRLD) mechanism.

6.3.4 Fast and Reactive Link-failure Detection

We implemented FRLD in our OPNET simulator and simulated the scenario depicted in Figure 6.2.a. The results are shown in Table 6.3.

We can see that T_{resume} is less than 36 seconds for FRLD's worst case if T_{NUD-PP} equals 30 seconds. This represents an improvement of 650% for link-failure detection and reaction compared to the default Contiki's best value. T_{resume} is around 205

FRLD overhead	DAO overhead	
	DTSN	NO DTSN
240	200	35

Table 6.4: Overhead induced with FRLD and with or without DTSN continuous increase.

seconds in the worst case of FRLD if T_{NUD-PP} is 240s. This still represents an improvement of 12% compared to Contiki's default behavior. In the best case, FRLD results in an improvement of 300% if T_{NUD-PP} is 240s. Figure 6.3 displays resuming time for both Contiki's default behavior and FRLD with T_{NUD-PP}=240s. We can see that FRLD provides resuming time less than T_{NUD-PP} value. Contiki resuming time is more scattered due to the fact that it highly depends on which node is going to send its DAO after a communication breakdown. If it is node 7, the communication will be resumed faster than if it is node 6, which explains the variance between 250s and 800s.

6.3.5 Consequences on signaling overhead

The performance of FRLD comes at the cost of adding signaling overhead as it requires the sending of neighbor solicitations (and the corresponding answers – neighbor advertisements) every T_{NUD-PP}. Table 6.4 summarizes the overhead added by FRLD. For one hour and twenty of simulated time, this corresponds to approximatively 240 NS-NA sent packets. The total overhead produced can be then expressed thanks to Equation 6.5.

$$FLRD_{overhead} = (T_{simu}/T_{NUD-PP}) * NB_{Nodes} - 1 \tag{6.5}$$

6.3.6 FRLD and DTSN

While Smart Grid devices are not energy constrained, it is still important to try to reduce the energy impact of FRLD. As described previously, Contiki increments DIO DTSN in a continuous fashion. This means that a huge amount of DAO messages are going to be sent while they are not providing any new or useful information. We saw that the fact that one DAO is emitted for each received DIO can lead to a minimum detection for link-failure. However, with FRLD, the continuous DTSN increase is no longer necessary – link breakdown detection is the only reason for the frequent increase of the DTSN. As Smart Grid utilities know the number of customers managed by a DC, they can decide to stop to increment DTSN once all downward routes are installed on the DC. Alternatively, by using P-4Dia, OM-4Dia or OA-4Dia (as discussed in Section 5.5) with the appropriate parameters, a DC

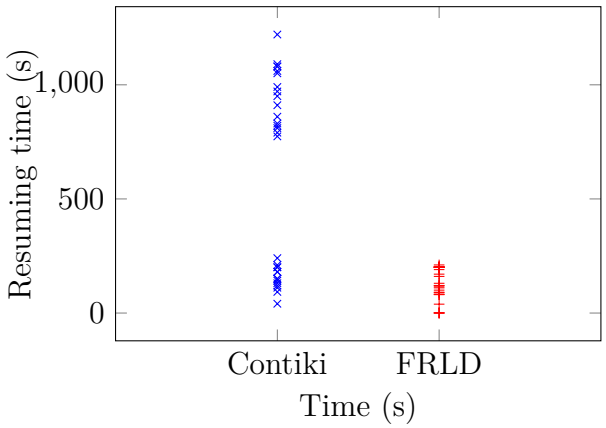


Figure 6.3: Resuming Time for Contiki and FRLD with $T_{NUD-PP} = 240s$ and S_{Off}=2900s. Results are given for 30 independent simulations with 30 different seeds.

can stop the continuous DTSN increase after a fixed period of time (e.g. 2 hours). The Equation 6.6 approximates roughly the number of DAOs that can be saved if DTSN is not incremented continuously.

$$DAO_{overhead} = ((T_{route} - Tsimu/I_{mean}) * (NB_{Nodes} - 1) * AverageRPLRAnk \quad (6.6)$$

I_{mean} stands for an approximation of Trickle timer that is going to trigger the emission of a DIO with an increased DTSN and thus to lead to the emission of a DAO. It could be roughly approximated with I_{mean} equal to the average value of I_{max} (1048s) and $I_{max}/2$ (524s).

Table 6.4 represents the overhead produced in case DTSN is not increased, compared to the case when it is increased. The number of prevented DAO messages is comparable to the overhead produced by FRLD (as NS-NA are 70 bytes and a DAO 63 bytes).

6.4 Related work

Being a RPL reference implementation, Contiki RPL has been widely investigated in the literature, mainly about performances in Wireless Sensor Network [TZW12], [DDB12], [GKPG14] and [GKC+12]. To the best of our knowledge, [RLP+] is the only paper focusing on ContikiRPL over PLC.

The author of [KG11] studied the interaction of RPL and NUD, where he evaluates the impact on neighbor cache entry lifetime on link failure detection with an analytical model. Due to the fact that Contiki uses infinite cache entry lifetime,

such method cannot be used in practice. Moreover, the analytical model provides interesting results but without validation, the applicability to a real-world scenario remains to be confirmed. In [TDOV10] Tripathi *et al.* analyzed RPL's behavior when link failures occur. They focused on local repair, i.e. the fact that a node is loosing any potential parent. Results are showing that local repair has the desired effects but link failure detection was not optimized.

6.5 Conclusion

We showed in this chapter that the ETX metric suffers from drawbacks when it comes to react and detect rapidly link-failure for specific AMI traffic patterns. Next chapter is going to present a novel designed metric specifically tailored for multi-modulation environment, such as IEEE P1901.2

6

7

A new metric for RPL: Channel Occupancy

The routing decisions in RPL are based on the abstract notion of OF, which uses a specific metric for the calculation of the position of each node in the DODAG. The protocol itself is independent of the metric, and can be applied to a wide variety of scenarios depending on the choice of the metric in question. Following the observation that collisions and channel fluctuation are some of the major reasons for degraded wireless network performance, the metric Expected Transmission Count (ETX) based on the average number of packet retransmissions became one of the most widely used. More specifically, in the majority of the studies in the literature, the default metric used for RPL evaluation is ETX, as shown in Table 3.2.

While this metric offers the advantage of measuring the path quality quite accurately, it has several drawbacks:

- [ITN13] showed that, while ETX is accurate to reflect the link quality, it is highly unstable and can lead to a lot of parent changes in the topology, which produces to high overhead;
- ETX is monitored only for the active links carrying traffic. In [DDB12], Darwarn *et al.* demonstrated that the choice of $INIT\_LINK\_METRIC$ is of crucial importance as a high value could lead to not consider parents with better link quality than the currently preferred one.

Moreover, the ETX metric does not reflect one of IEEE P1901.2's main functionalities: it uses several modulations, each providing different throughput and range.

In this chapter, we introduce our proposal for a new metric for RPL: the *Channel Occupancy* (CO) metric that takes into account the existence of multiple nominal throughputs over a given interface. The metric aims at minimizing the channel occupancy time instead of trying to reduce the Expected Transmission Count. Although in many of the existing networks the two are directly related, in IEEE P1901.2 the relation is not linear. We present results obtained for the CO metric compared to ETX. In addition, we present a comparison of the results to the performance of two other routing protocols for *Low power and Lossy Network* (LLN): *6LoWPAN Ad Hoc On-Demand Distance Vector Routing* (LOAD) and *Lightweight On-demand Ad hoc Distance-vector Routing Protocol Next Generation* (LOADng).

Finally, we introduce a novel proactive link-estimation technique – *Channel Occupancy Active link-estimation* (COALE). This technique allows us to profit from the full benefits of candidate parents and do not rely uniquely on the preferred parent. This is done through the introduction of the notion of DIS-NA messages, a slightly modified version of DIS message.

7.1 Problem Statement

ETX is a well-known, popular metric, which possesses very good characteristics. However, when dealing with a graph topology (such as RPL) and not restricting to a tree topology, the variety of potential parents is underused. The ETX to the preferred parent will always be estimated in a more active manner, while alternative routes are neglected. Moreover, when the characteristics of a link can be chosen and can vary significantly in terms of nominal bandwidth and packet error rate, the ETX metric is completely inadequate.

Both of these situations occur frequently in an IEEE P1901.2 network with proactive routing with RPL.

In order to illustrate the two cases when ETX provides suboptimal results, we provide a simplified example. Let's consider the DODAG of the topology depicted in Figure 7.1(a). We are interested in node 5's preferred parent choice. There are two possibilities:

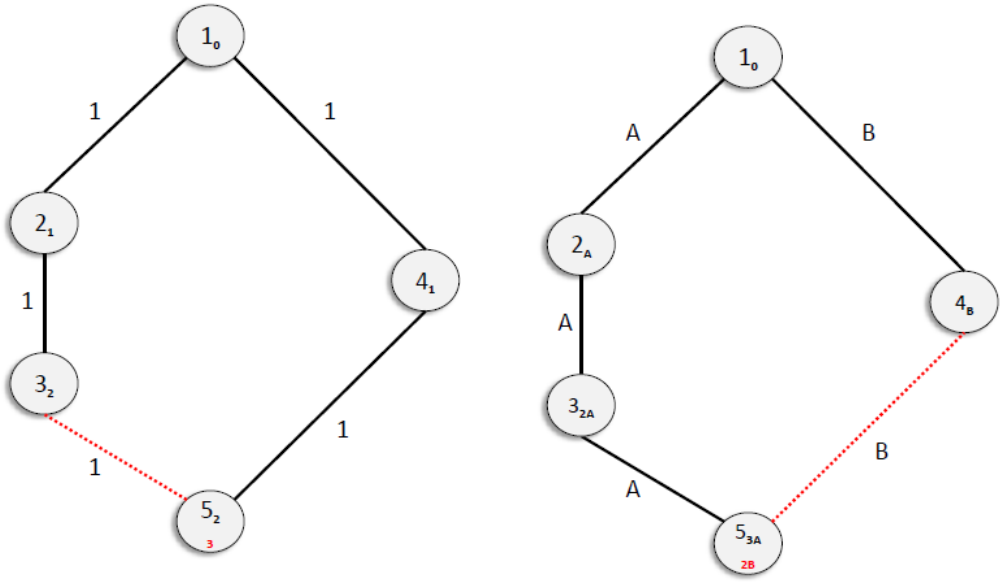
1. $5 \Rightarrow 3 \Rightarrow 2 \Rightarrow 1$
2. $5 \Rightarrow 4 \Rightarrow 1$

Using ETX as metric will result in node 4 as preferred parent for node 5 (the ETX from node 4 is less than the ETX from node 3). However, this selection is optimal only if the available modulations provide comparable throughputs. Figure 7.1(b) depicts the same topology but instead of using ETX as a metric, the nominal throughput of the available modulation is used. If we denote by A and B the two modulations having respectively a link cost of A and B, the path cost for node 5 will be:

1. $3A$ for the path $5 \Rightarrow 3 \Rightarrow 2 \Rightarrow 1$
2. $2B$ for the path $5 \Rightarrow 4 \Rightarrow 1$

If modulation A is twice as fast as modulation B, the normalized cost of A will be 1, while the cost of B would be 2. The cost of selecting the first path (via node 3) would be 3, whereas the one via node 4 would be 4. The optimal solution for node 5, and behavior for the network, would be to prefer node 3 instead of node 4. Note that the relation between ETX and the latter case is not straightforward – even though the packet error rate is correlated with the modulation (e.g. a faster modulation leads to shorter transmission times), the required SNR also changes, which makes a direct comparison non-trivial. ETX does not always provide the best route selection

criteria, particularly in environments using several modulations. When the environment under question is limited in resources (e.g. energy, throughput) not wasting them is of particular importance. A new metric thus needs to be defined in order to take into account the particularities of these multi-modulation technologies for low-powered, lossy networks.



(a) ETX (b) Modulation

Figure 7.1: DODAG construction based on ETX or modulation.

7.2 The Channel Occupancy metric

The *Channel Occupancy* (CO) metric is inspired from the Airtime metric defined for mesh networks. IEEE 802.11s defines Airtime as "a duration computed regarding to the modulation used for a test frame of 1Kbyte and according to probability of frame corruption". Airtime tends to minimize the global channel occupation by taking into account both the throughput and frame corruption.

By analogy, we defined the CO metric for RPL as "the time needed to send a frame of 100 bytes". It can be used for both OF0 and MRHOF Objective Functions. In addition to taking into account solely the different available modulations, however, CO takes into account the possibility to ignore a subset of the available bandwidth because of noise interferences (e.g. Tone-Mapping).

The CO metric is calculated from the time needed to transmit a frame. It integrates the Tone-Map mechanism (Section 2.3.3) in order to estimate the modulation (and the number of activated sub-bands) to use with a given destination. The IEEE P1901.2 Tone-Map mechanism operates in a reactive way, i.e. the sub-band and

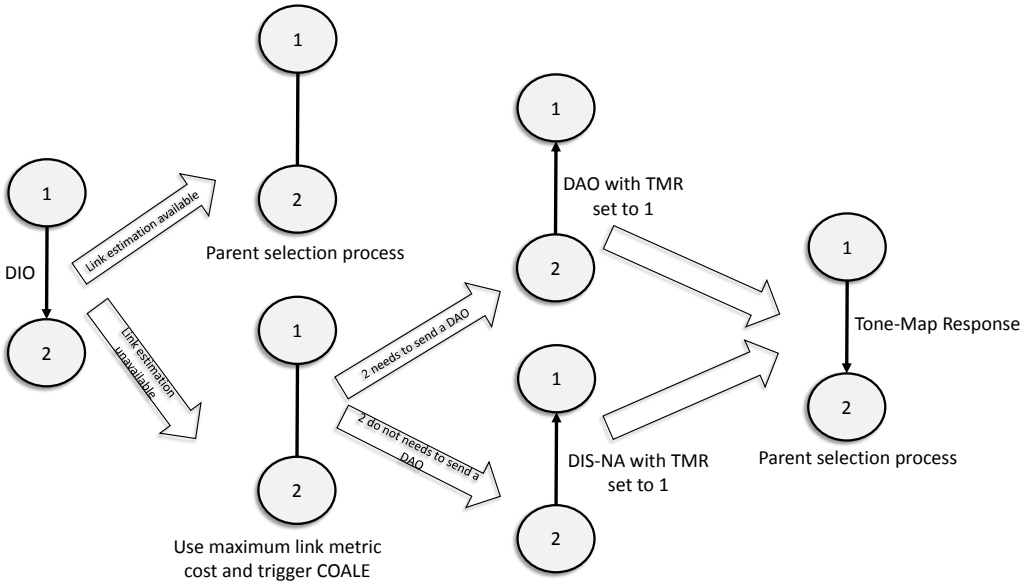


Figure 7.2: Channel Occupancy implementation

modulation to use are estimated and known only if data traffic has to be sent to a given destination.

However, if we want to minimize the channel occupancy (and thus have an optimal network performance), we need to proactively probe the channel to all parents of each node. To that purpose, we propose an active link-estimation technique for candidate parents: *Channel Occupancy Active link-estimation* (COALE). Please note that a node A is a candidate parent for a given node B if its rank is less than the given node rank (e.g. $rank(A) < rank(B)$). We provide a detailed description of COALE in Section 7.2.1.

During the lifetime of a network, the modulation to be used along with the Tone-Map are determined from measurements of data packet transmission parameters or proactive COALE estimation to the list of candidate parents. If the modulation to use with a given neighbor is unknown the link cost is set to $ChannelOccupancy_{InitLinkMetric}$, which corresponds to ROBO modulation *link_cost*.

7.2.1 Channel Occupancy with active link estimation

In this thesis we introduce for the first time *Channel Occupancy Active link-estimation* (COALE). The role of Channel Occupancy Active link-estimation (COALE) is to monitor candidate parents' link-quality. This information is used to reevaluate the usable modulation and Tone-Map characteristics not only to the preferred parent, but to the whole set of possible RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) parents. This point is crucial for taking full

advantage of the path diversity of the DODAG structure built by RPL.

Figure 7.2 depicts the CO mechanism. When a node receives a DIO message with rank less than its own and it does not know neither the modulation, neither the sub-bands to use, it triggers the COALE mechanism for the newly identified node. COALE is based on periodical message emission, which in the absence of traffic to a given node allows to keep up to date the physical layer information (modulation, Tone-Map). However, we want to keep the networking stack as simple as possible, avoiding cross-protocol interactions whenever possible. For that purpose, we define a new type of message – the *DIS No Answer* (DIS-NA). DIS-NA is a normal RPL DIS message, with an optional optimization added to the way it is processed as to improve the network performance. Indeed, DIS-NA is a slightly modified DIS, with the only difference being to specify to the DIS-NA receiver that it does not need to answer with a DIO.

The usage of DIS-NA allows to save 2 message transmissions on the network – the unicast DIO sent in response to a unicast DIS and its acknowledgment. DIS-NA messages are sent with the TMReq bit is set to 1 which will trigger a Tone-Map response from the DIO's sender that will permit to obtain modulation and sub-band information update. In addition, it will trigger the parent selection with the CO metric. Algorithm 11 presents COALE's behavior.

Algorithm 11: COALE

Node B sends a DIO to Node A
Node B has a rank smaller than Node A
if (Node A knows the modulation and sub-bands to use with Node B) **then**
  Trigger CO metric's parent selection procedure with Node B modulation and sub-bands activated
else
  Trigger CO metric's parent selection procedure with Node B with $ChannelOccupancy_{InitLinkMetric}$
  Trigger DelayDisNA
end if
DIS-NA Sending:
if DelayDisNA is expired **then**
  Send DIS-NA
end if
TM-Response received:
Trigger CO's metric parent's selection procedure with Node B and information contained in TMResp

In order to avoid DIS-NA storm that could happen when multiple nodes receive the same DIO with a rank less than theirs, emission of DIS-NA must be carefully managed. We used a similar approach as 4Dia, which we introduced in Section 5.3.

At the reception of a DIO with smaller rank, a timer *DelayDisNA* is armed. This timer must take into account that a DAO message can be sent at the reception of a DIO message from preferred parent. Then, two cases can occur. If the sender of the DIO is the preferred parent and the node should generate a DAO, or if the sender of the DIO is a candidate parent. In the former case, the emission of a DIS-NA will be canceled as the DAO message will allow to estimate the link-quality while in the latter case, DIS-NA is sent after the expiration of *DelayDisNA*. Algorithm 12 describes the *DelayDisNA* timer management. Similarly to 4Dia, DIS-NA acknowledgments are used to tune *DelayDisNA* emission.

Algorithm 12: DelayDisNA management

if (Node A needs to send a DAO to Node B i.e. Node A is Node B's preferred parent) **then**
  Do Nothing
else
  Trigger DelayDisNA
end if
with DelayDisNA = (DelayDisNAMin;DelayDisNAMax)

7.2.2 Channel Occupancy expression

The CO expresses the channel occupation time needed for sending a 100 bytes data frame. Thus, *Channel Occupancy* (CO) is the time needed to send the data frame but also to send the subsequent acknowledgment (Equation 7.1).

$$Total_{ChannelOccupancy} = T_{100Bframe} + T_{ACK} \tag{7.1}$$

From Equation 7.1 we can compute the channel occupancy depending on modulation and number of activated sub-bands, as shown in Table 7.1.

We can use the duration values presented in Table 7.1 as a basis to determine the possible values for the Objective Function metric.

7.3 Channel Occupancy for OF0

OF0 comes with the assumption that metric's quality should be an integer between 1 and 9 (excellent to worst). The sending time of a data frame of 100 bytes (computed in Table 7.1) normalized to values between 1 and 9 is given in Table 7.2.

OF0 does not need to be further modified in order to use CO as metric (see Section 3.3.3.1 for a detailed description of OF0).

Activated Sub-bands \ Modulation	D8PSK	DQPSK	DBPSK	ROBO*
6	0,0491	0,0547	0,0728	0,1715
5	0,0516	0,0583	0,0800	
4	0,0554	0,0637	0,0908	
3	0,0617	0,0728	0,1089	
2	0,0742	0,0908	0,1451	
1	0,1117	0,1451	0,2535	

Table 7.1: Channel Occupancy durations (in s) for a 100B frame. (* the ROBO modulation always uses all sub-bands)

Activated Sub-bands \ Modulation	D8PSK	DQPSK	DBPSK	ROBO*
6	1	1	2	6
5	1	1	2	
4	1	2	3	
3	1	3	3	
2	2	5	5	
1	3	9	9	

Table 7.2: Channel Occupancy metric values with OF0. (* the ROBO modulation always uses all sub-bands)

7.4 ChannelOccupancy for MRHOF

The situation with CO for MRHOF is slightly different than the case of OF0. The metric value is not bounded between 1 and 9. However, a major requirement of RPL standard is that the rank increase could not be less that *MinHopRankIncrease*. While this requirement is satisfied "by default" for OF0 (the link quality being multiplied by *MinHopRankIncrease* during the rank computation), with MRHOF the metric must be managed carefully in order to respect that requirement. *MinHopRankIncrease* restrics "de facto" the maximum number of hops reachable in the network. By default, *MinHopRankIncrease* is set to 256 (see RFC 6550 [WTB+12]). As the rank in RPL is encoded in 16-bits, this leaves us with a maximum number of 256 hops. The smallest maximal number of hops can be calculated from Equation 7.3 as it is bounded by the metric's maximum value.

$$NumberOfHop_{MIN} = 65536/MAX\_LINK\_METRIC \tag{7.2}$$

This strong relationship between *MinHopRankIncrease*, maximum number of hops and maximal value for a metric imposes strong limitations on the way the maximal value for a given metric is chosen. Given that IEEE P1901.2 can use 4 modulations and 6 sub-bands, this gives 19 distinct combinations to characterize (as the ROBO modulation always uses all sub-bands). This means that if we use the default *MinHopRankIncrease*, the best modulation and sub-band combination (D8PSK with 6 sub-band activated) must have a value of 256.

Note that *MinHopRankIncrease* is also used for rank computation (Section 3.3.3.1). Two nodes are considered to have the same rank if the DAGRank function (given in Equation 7.3) computes the same results for the two. The consequence is that the ranks of two nodes must differ with at least *MinHopRankIncrease* to be considered to have a different rank. Thus, considering that we have to express 19 metric values needed for CO, a rank increase of 4864 (256×19) is needed in order to be able to distinguish the rank between the best and the worst metric values. This gives a maximum of 13 hops, which is insufficient in an AMI environment. We decided to use a *MinHopRankIncrease* of 10 and to normalize the CO metric between 10 and 256 which results in the smallest maximum number of hops of 256. Table 7.3 gives the CO metric values used with MRHOF. These values are computed from Table 7.1.

$$DAGRank_{(rank)} = floor(rank/MinHopRankIncrease) \tag{7.3}$$

We can see by comparing Table 7.2 and Table 7.3 that MRHOF allows a more precise characterization of the link, e.g. OF0 does not discriminate between 6 and 3 sub-channels with D8PSK, contrary to MRHOF.

MRHOF introduces an hysteresis function that helps to prevent parent change

Modulation / Activated Sub-Band	D8PSK	DQPSK	DBPSK	ROBO*
6	10	17	38	158
5	13	21	47	
4	18	28	60	
3	25	38	82	
2	40	60	125	
1	85	125	256	

Table 7.3: Channel Occupancy metric values with MRHOF. (* the ROBO modulation always uses all the Sub-Bands)

for small metric variations. For our evaluations, we set the hysteresis value of CO metric to 5.

7.5 Channel Occupancy and ETX

While the CO metric guarantees the usage of best path in term of minimizing the channel occupation, it remains important to take into account the link-quality in terms of reliability. To that purpose, we integrated ETX to the parent selection process. ETX has two roles:

- in case two candidate parents have the same CO metric value, ETX is used as a tie-breaker as described in Algorithm 13;
- if the ETX value is too high for a given candidate parent, it is must not be selected. We introduce a new threshold to fine-tune this behavior – *MAXIMUM_ETX_THRESHOLD*. For our simulations we used the default value of 3, i.e. if ETX to a preferred parent is greater than 3, the node must not select the candidate parent as a parent. This rule is in effect only in the case there is more than one candidate parent.

Algorithm 13: Usage of ETX with CO metric

Node C is the candidate parent, Node A is executing the parent selection and has Node P as a preferred parent
if (Node A ETX with candidate Parent C > MAXIMUM_ETX_THRESHOLD) **then**
  Do not select Node C except if it is the only candidate parent
else if (Node C CO metric == Node P CO metric) **then**
  Select as a parent the node with minimum ETX between Node C and P
end if

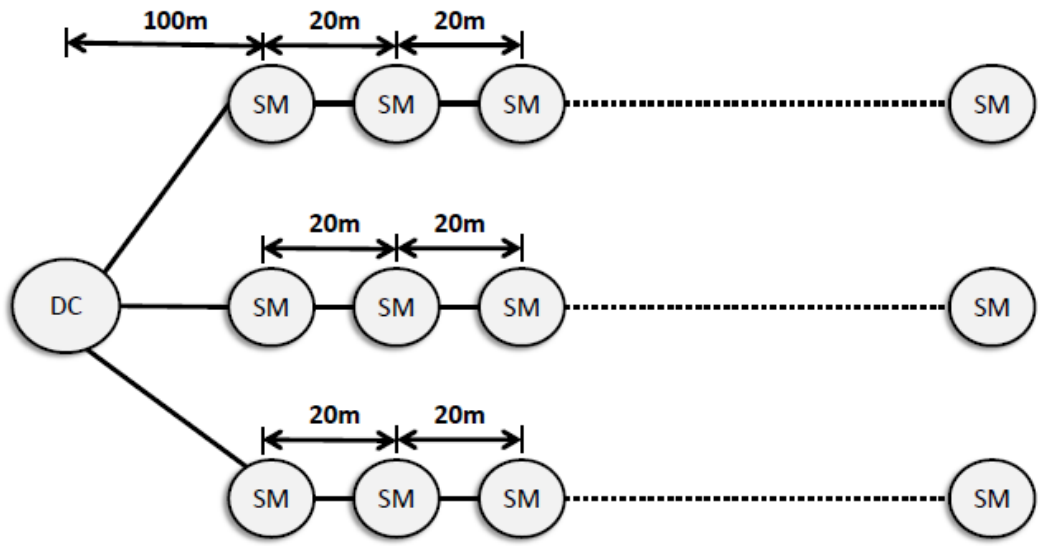


Figure 7.3: Large-scale three-phased testbed.

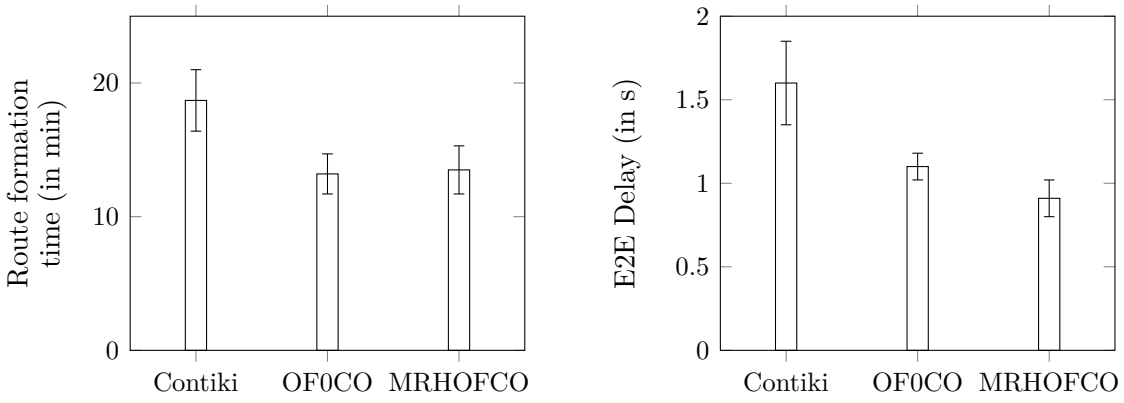
7.6 Performance evaluation – Channel Occupancy vs vanilla Contiki (MRHOF with ETX)

In order to evaluate the performance of the CO metric, we use the large-scale testbed depicted in Figure 7.3. This topology emulates a three-phased LV AMI network with 133 SMs per phase and one DC in charge of collecting the data. CO is compared to vanilla Contiki's Expected Transmission Count implementation with Minimum Rank with Hysteresis Objective Function OF. Table 7.4 summarizes the parameters used for the simulation.

Parameter	**Value**	
Number of nodes	400	
Trickle	Min Interval [2;4s] - Max Interval [524;1048s]	
DelayDAO	[4;12s]	
Traffic Pattern	100 bytes packet every [0;900s] froms SM to DC	
Vanilla Contiki	**Objective Function**	MRHOF
	Metric	ETX
Channel Occupancy	**Objective Function**	OF0
		MRHOF
	Metric	CO

Table 7.4: Simulation parameters

In that scenario, each SM starts sending 100 byte packets to the DC after $1H$ of simulated time using an uniform distribution between 0 and $900s$.



(a) Route Formation time.

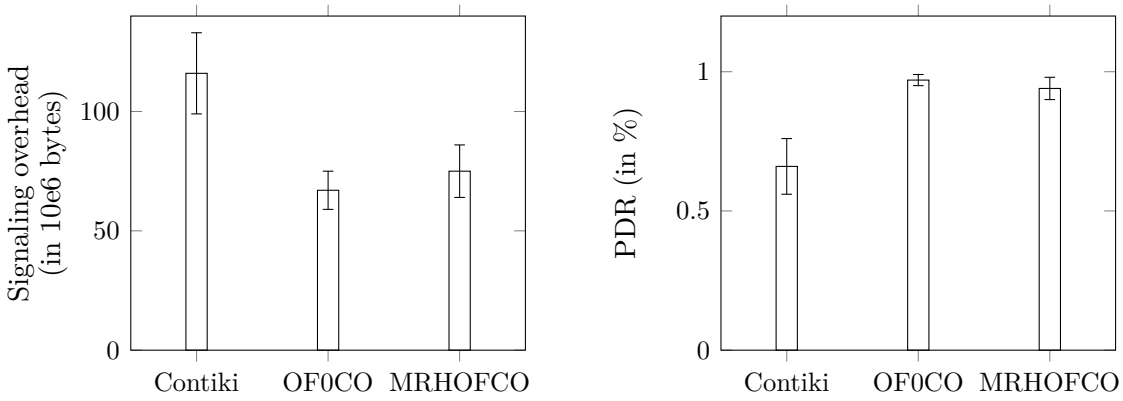
(b) End-to-End (E2E) delay.

Figure 7.4: Route formation time and E2R delay in a large-scale narrowband PLC network with RPL under different objective functions – vanilla Contiki (with ETX/MRHOF), OF0 based on CO, and MRHOF based on CO. The bars provide the average values over 30 independent simulations, whereas the whiskers indicate the 95% confidence interval.

In order to compare vanilla Contiki and CO metric, we are going to observe a set of metric for 30 runs of $24H$ of simulated time: Route Formation Time, Signaling overhead (number of DIOs and DAOs sent), *Packet Delivery Ratio* (PDR), *End-to-End* (E2E) delay, hop-count, and DODAG stability.

Figure 7.4(a) depicts route formation time for vanilla Contiki (ETX/OF0, and CO for both OF0 and MRHOF. Route formation for both CO-based methods takes approximately the same time (around 13.5 minutes) while Contiki takes 50% more (6 additional minutes). This is due to ETX's behavior during the route formation process. As described in Section 6.1, the value of ETX increases in case of unsuccessful DAO transmission, whatever the reason – be it collisions (and therefore dropped packets) or bad-quality link. Thus, a short burst of collisions may significantly increase the ETX of the link to the preferred parent, and eventually – trigger DODAG reconfigurations. This in turn generates additional signaling messages, putting the network in a chain of reconfigurations, which explains the differences in route formation time.

Figure 7.4(b) shows the average E2E delay observed at the DC. We can notice than CO with MRHOF provides the best E2E delay with an improvement of 43% compared to Contiki and 17% compared to CO with OF0. The difference between CO OF0 and CO MRHOF is explained by the difference in the design of the two solutions. CO MRHOF allows more precise characterization of the link quality by expressing the CO metric on a wider range. This in turn allows to select the most efficient path, while CO OF0 guarantees the usage of a route that is estimated as sufficiently good. For Contiki E2E delay, the difference is explained by ETX metric's



(a) RPL signaling overhead.

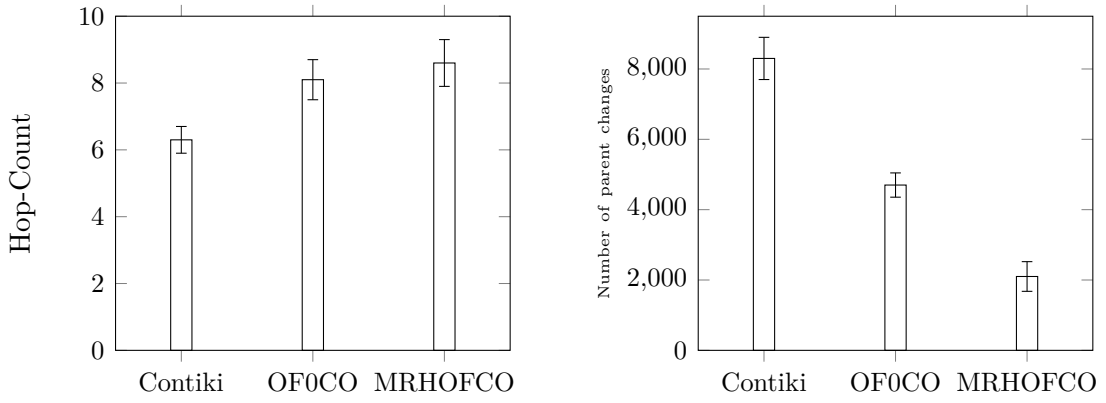
(b) PDR observed at the DC.

Figure 7.5: Average values and 95% confidence interval for signaling overhead and PDR with RPL different metrics – vanilla Contiki (with MRHOF), OF0 based on CO, and MRHOF based on CO.

intrinsic behavior. IEEE P1901.2 does not implement an RTS-CTS mechanism, and this leads to a considerable amount of collision in the network. This results in bursty ETX increases and subsequent topology changes. This is a drawback of ETX in environment with dense node deployment with no inherent mechanism to avoid the hidden node problem. Sometimes, it would be preferable to accept (e.g. ignore) the loss of some packets instead of changing the topologies in reaction. A possible approach would be to adjust the time-weighting coefficient as a function of the number of neighbors, i.e. high-density regions would put more weight in the historical values, while low-density ones could allow to be more reactive.

Figure 7.5(a) confirms the observation that ETX tends to generate more DODAG reconfigurations and thus to generate more signaling messages. Indeed, vanilla Contiki (ETX with MRHOF) is producing almost twice the overhead than CO MRHOF and CO OF0. We can also notice than CO OF0 is producing 25% less overhead than CO MRHOF. This result is due to the fact that CO MRHOF seeks to fully optimize the link quality, and assigns more distinct values to the different combinations of modulation/sub-channels compared to CO OF0. As shown in Figure 7.5(b), Contiki is offering the lowest PDR. Once again, reconfiguration due to ETX increase leads to instability in the network and to non-negligible increase in the number of dropped packets.

We can observe that vanilla Contiki is offering the best performance in terms of hop-count in Figure 7.6(a) (e.g. lowest number of hops). As CO minimizes the channel occupation, it tends sometimes to select longer path, but with fastest modulation. The results are thus consistent to the expected behavior of ETX vs CO. The number of parent changes in the network (Figure 7.6(b)) reconfirms our observation that vanilla Contiki is overreacting to packet collisions, thus resulting



(a) Hop-Count observed at the DC

(b) Number of parents changed in the network.

Figure 7.6: Average values and 95% confidence interval for hop-count and number of parent changes with RPL different metrics – vanilla Contiki (with MRHOF), OF0 based on CO, and MRHOF based on CO.

in higher number of parent changes.

RPL with CO metric clearly outperforms vanilla Contiki implementation. Offering better stability and taking into account the multi-modulation scheme, it permits to lower E2E delay as well as maximizing PDR.

7.7 Comparison to reactive routing protocols for LLN: LOAD and LOADng

.

In addition to comparing RPL with our proposed metric *Channel Occupancy* (CO), we wanted to evaluate how it ranks against its reactive counterparts – LOAD and LOADng. Multiple comparisons between these protocols exist (see Section 3), with the results depending strongly on the underlaying assumptions and the parameters chosen for the studies.

Parameters	LOAD	LOADng
Route Lifetime	1H	
Net Traversal Time	10s	
RREQ_RATELIMIT	2	
RRER_RATELIMIT	2	
Metric	Hop-Count	
Traffic Pattern	100 bytes packet every [0;900s] froms SM to DC	

Table 7.5: LOAD and LOADng parameters

We performed 30 simulations with 30 different seeds for the topology already used to evaluate CO metric with the same traffic pattern (Figure 7.3). We chose the parameters accordingly, and are provided in Table 7.5 for LOAD and LOADng. LOAD and LOADng use hop-count as their default metrics, whereas RPL was evaluated with our proposed CO metric.

Parameters	RPL		LOAD	LOADng
	OF0	MRHOF		
Signaling Overhead (10e6 bytes)	67 ± 8	75 ± 11	45 ± 5	90 ± 9
Average E2E delay	$1.1s \pm 0.08$	$0.91s \pm 0.11$	3.6 ± 0.14	3.42 ± 0.06
PDR	0.97 ± 0.02	0.94 ± 0.04	0.76 ± 0.06	0.69 ± 0.09
Hop-Count	8.1 ± 0.6	8.6 ± 0.9	7.5 ± 1.2	6.7 ± 0.8

Table 7.6: Performances comparison between RPL, LOAD and LOADng

7

7.7.1 LOAD and LOADng

We can see on Table 7.6 that the E2E delay is almost identical for LOAD and LOADng, with negligible advantage for the latter. This is mainly due to the traffic pattern. With an inter-arrival time between 0 and 15 minutes, each SM sends on average 8 packets per hour. As route lifetime in LOAD and LOADng is set to one hour, route discovery process is performed once every hour. Thus, 1 packet in 8 takes suffers the route establishment phase. LOADng improvements do not allow to improve E2E delay with such traffic pattern.

Regarding average hop number from packets received at the DC, we can see that LOADng allows to reduce number of hops needed to reach the DC. However, E2E delay remains comparable for both solutions. In fact, LOADng improvements (i.e. allow forwarding of route request already received to find better routes) trigger more flooding and as a consequence – collisions, which results in higher overhead (LOADng's overhead is almost twice as LOAD's) and smaller PDR.

7.7.2 LOAD, LOADng and RPL

We can see in Table 7.6 that RPL with CO metric outperforms LOAD and LOADng regarding the E2E delay. When signaling overhead is concerned, LOAD offers the best performance while it is interesting to notice that LOADng produces more overhead than RPL with CO metric. PDR is giving different results. As RPL

permits to obtain satisfying PDR, LOAD LOADng do not allow to obtain PDR better than 76%. Hop-Count is minimized by LOAD and LOADng.

Comparisons always need to be performed carefully. The results obtained for the comparison of LOAD, LOADng and RPL clearly show that RPL with CO metric performs better. However, as shown in Section 3.3, opposite results could be obtained by changing some parameters configuration. The goal of these comparisons was to use a minimal version of reactive routing protocols and to analyze differences obtained in the results in order to validate the CO metric.

7.8 Conclusion

In that chapter, we introduced a novel metric to be used with RPL: the *Channel Occupancy* (CO) metric. To the best of our knowledge, this metric is the first to be introduced that takes into account multi-modulation scheme. Being designed in a generic fashion, this metric could be extended to any other environment which can benefits from multi-modulation.

7

8 Conclusion and perspectives

In this chapter, we will remind the addressed problems, put in emphasis the solutions and our contributions, and finish with perspectives.

8.1 Conclusion

The purpose of our thesis was to study RPL's behavior in SG architecture and more particularly for Advanced Metering Infrastructure communications. To that purpose, we developed a complete AMI architecture simulator in OPNET. This simulator, presented in Chapter 4, not-only includes higher-layer communication stack, but also a modular physical model that permits to emulate PLC's channel behavior with the desired granularity. We validated that simulator against a real-testbed and we showed that our simulator allows to emulate a real environment.

RPL has been defined specifically for *Low power and Lossy Network* (LLN). As we showed in this thesis, LLN is not a single kind of network: from *Wireless Sensor Network* (WSN) to PLC Smart Meter environment, there are differences that need to be taken into account. It leads to the fact that RPL is a very complex protocol to handle and time is needed to completely master its for specific environment. This is why we proposed several optimizations to RPL for IEEE P1901.2 environment. We decided to based our work on a RPL timely iterative approach, RPL beings made of several phases: from RPL startup to RPL steady-state.

We started by enhancing the startup phase of RPL in Chapter 5. To that purpose, we introduced a new DAO emission management system: 4Dia. By eluding at maximum dynamically the congestion due to Destination Advertisement Object messages, this mechanism permits to guarantee faster RPL convergence for the Smart-Grid i.e. all the Smart Meters are going to be reachable faster.

Then, in Chapter 6, we took into account one of on the Smart Grid specificity: its bidirectionality requirement – communications from Data Concentrator to the Smart Meters can be as important as communications from the Smart Meters to the Data Concentrator. To that extent, we highlighted that RPL may suffers from long period of SM unreachability in case of link-breakage because of SG traffic pattern. To that purpose, we introduced FRLD that allows to resume communications faster

by speeding-up the link-failure detection, and to react faster to construct the needed topology to overcome the link-breakage.

Finally, in Chapter 7, we introduced a brand new metric for RPL: the *Channel Occupancy* (CO). This metric, adaptable to any physical layer offering several modulations, allows to reduce physical channel occupation by computing path based on the modulation used. CO metric allows to improve E2E delay while guaranteeing a better stability compared to the reference ETX metric. In this chapter, we also compared RPL with two other routing protocols: LOAD and LOADng. These two protocols clearly show worse performances but we did not seek to optimize their performances specially for SG in that thesis.

8.2 Perspectives

While this thesis enhanced RPL for IEEE P1901.2, works remains to be done in order to have a complete optimized version of RPL.

8.2.1 Real on-the-field experimentations

While we validated our implementation regarding to a testbed, nothing can replace real on-the-field experimentations. Model used in simulation can mimic the reality to a certain extent but real-testbed experimentations could help to tailor even better the protocol. Moreover, the Smart Grid remains a quite close world as shown by the lack of existing literature on typical traffic pattern used in AMI. Only utilities real-testbed could help to perform the ultimate optimizations.

8.2.2 Multiple Technology Management

SMs are long-live equipment and utilities started to imagine the possibility to integrate several technologies on the same SM. Having wireless technologies could help to overcome the drawbacks of PLC and conversely. Thus, it would be important to study RPL behavior in that case. Two possibilities can be imagined:

- using a Medium Access Shared layer between the physical and the MAC layer in order to turn the fact to have two technologies transparent;
- using several RPL instances and let RPL manage by itself the two technologies.

8.2.3 Composite Metric

While we have shown that CO can guarantee good performances in SG environment, it would be important to develop composite metrics, i.e. metrics that take

into account more than one criteria. In CO, we used ETX as a tie-breaker, but it would be interesting to have a single metric integrating several parameters.

8.2.4 Hybrid approach

RPL is clearly efficient for managing upward route. Downward routes, being optional and not the main objective, remain suboptimal. Indeed, routes are constructed regarding the upward link-cost. Instead of using RPL for downward route management, it could be interesting to use a proactive protocol like LOADng or to use opportunist routing.

8

A

LOAD and LOADng differences

LOAD and LOADng constructs routes based on Route Cost. When a RREQ is received by the destination, if the metric value is less than the one already received for the same RREQ, a new RREP message is sent back to the source. LOAD uses only one metric to optimize routes: the hop-count while avoiding weak link (a weak link is a node whose LQI is less than a threshold). While LOADng use that metric by default, it adds the possibility to use arbitrary additive metrics, which must be specified as extensions of LOADng. At present, no other metrics are existing for LOADng protocol.

LOADng adds an additional type of message: the *Route Reply - Acknowledgment* (RREP-ACK). The RREP-ACK is sent in response to a RREP message and must be asked explicitly by the sending node of the RREP. It allows to validate the bidirectionality of the route.

Data set management such as Routing Table and path information are managed in a different way. In LOAD, two databases have been defined:

- Routing Table Entry: which contains routing information concerning routes that had been established and that are currently in use. This table consists of:
  1. The destination address
  2. The next hop address
  3. The status (valid, invalid, route_discovery)
- Route Request Table Entry: which contains the temporary information about the path that is being established.

In LOAD, there is only one routing table. This means that the routing table is always updated using the information from the route discovery procedure. In other words, both the originator and the destination use the same route in both directions; which is not always optimal. This flexibility i not possible in LOAD protocol while in LOADng, another table has been introduced, the *routing set* apart from the routing table. The former contains the path search information and the latter contains routing information and is optionally updated with the Routing Set information. The Routing Set contains the following information:

- Route_Destination_Address: the address of one of the router interfaces or

the address of a node for which the router is responsible, that is, a node which is in an other domain and uses the router to connect to the MANET network.

- Route_Next_Address: the address of the next hop in the routing path.
- Route_metric_Type: the type of the metric that has been used right now to calculate the metric from the originator to the current node.
- Route_Metric: the metric of the path from the originator to the current node. LOADng allows a 16 bits metric field while LOAD allocates just 8 bits. This results in a better resolution while comparing the metrics and a higher number of hops to be accumulated while calculating the metric.
- Route_Hop_Count: the number of hops accumulated from the originator to the current node. In LOADng messages, we find both the Route_Metric and the Hop_Count, the latter being or not used in the metric calculation. In case one intermediate node doe not support a specific metric, it can switch easily to the default metric (hop count).
- Local Interface Set: which contains a list of all the router's interfaces, one interface having at least one address.
- Blacklisted Neighbor List: contains the list of neighbors to which the link has been detected to be unidirectional. More specifically, the following mechanisms can be used to infer that a link is unidirectional:
  1. Some L2 triggers, when the transmission of a packet fails.
  2. Some ICMP protocols, such as Neighbor Discovery Protocol.
  3. The absence of a RREP acknowledgment.
  4. The absence of a transport layer acknowledgment.

  Saving this information in LOADng avoids the selection of the same broken link and hence renders the protocol more efficient and the delay lower.
- Destination Address Set: contains the nodes' addresses which do not belong to the ad hoc routing domain and are connected to it via this router. This router is responsible for the reception of RREQ messages destined initially to those nodes and the generation of the corresponding RREP responses.
- Pending Acknowledgments Set: contains the RREQ information for which corresponding acknowledgment has not yet been received.

List of Figures

List of Tables

Bibliography

[ABC12] E. Ancillotti, R. Bruno, and M. Conti. Rpl routing protocol in advanced metering infrastructures: An analysis of the unreliability problems. In *Sustainable Internet and ICT for Sustainability (SustainIT), 2012*, pages 1–10, Oct 2012. 37, 38, 40, 41

[ABC13] E. Ancillotti, R. Bruno, and M. Conti. The role of the rpl routing protocol for smart grid communications. *Communications Magazine, IEEE*, 51(1):75–83, January 2013. 37, 38, 40, 41

[ABC14a] Emilio Ancillotti, Raffaele Bruno, and Marco Conti. Reliable Data Delivery With the IETF Routing Protocol for Low-Power and Lossy Networks. *IEEE Transactions on Industrial Informatics*, 10(3):1864–1877, August 2014. 37

[ABC+14b] Emilio Ancillotti, Raffaele Bruno, Marco Conti, Enzo Mingozzi, and Carlo Vallati. Trickle-L²: Lightweight link quality estimation through Trickle in RPL networks. *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014*, pages 1–9, June 2014. 37, 38, 41

[AGBC11a] N. Accettura, L.A. Grieco, G. Boggia, and P. Camarda. Performance analysis of the rpl routing protocol. In *Mechatronics (ICM), 2011 IEEE International Conference on*, pages 767–772, April 2011. 37, 38, 40

[AGBC11b] N. Accettura, L.A. Grieco, G. Boggia, and P. Camarda. Performance analysis of the rpl routing protocol. In *Mechatronics (ICM), 2011 IEEE International Conference on*, pages 767–772, 2011. 58

[BBCF13] A. Barbato, M. Barrano, A. Capone, and N. Figiani. Resource oriented and energy efficient routing protocol for ipv6 wireless sensor networks, Oct 2013. 37

[BBP10] A. Brandt, J. Buron, and G. Porcu. Home Automation Routing Requirements in Low-Power and Lossy Networks. RFC 5826 (Informational), April 2010. 26

[BDK+14] O. Balmau, D. Dzung, A. Karaagac, V. Nesovic, A. Paunovic, Y.A. Pignolet, and N.A. Tehrani. Evaluation of rpl for medium voltage

power line communication. In *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*, pages 446–451, Nov 2014. 36, 37, 38

[CLCL13] Lin-Huang Chang, Tsung-Han Lee, Shu-Jan Chen, and Cheng-Yen Liao. Energy-Efficient Oriented Routing Algorithm in Wireless Sensor Networks. *2013 IEEE International Conference on Systems, Man, and Cybernetics*, pages 3813–3818, October 2013. 37, 41

[CTGC+10] C. Chauvenet, B. Tourancheau, D. Genon-Catalot, P.-E. Goudet, and M. Pouillot. A communication stack over plc for multi physical layer ipv6 networking. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pages 250–255, Oct 2010. 36, 37

[DCABM03] Douglas S. J. De Couto, Daniel Aguayo, John Bicket, and Robert Morris. A high-throughput path metric for multi-hop wireless routing. In *Proceedings of the 9th Annual International Conference on Mobile Computing and Networking*, MobiCom '03, pages 134–146, New York, NY, USA, 2003. ACM. 6, 72

[DCTS12] Niccolo De Caro, Walter Colitti, Abdellah Touhafi, and Kris Steenhaut. Comparative performance study of RPL in Wireless Sensor Networks. *2012 19th IEEE Symposium on Communications and Vehicular Technology in the Benelux (SCVT)*, pages 1–6, November 2012. 37, 39, 40

[DDB12] S. Dawans, S. Duquennoy, and O. Bonaventure. On link estimation in dense rpl deployments. In *Local Computer Networks Workshops (LCN Workshops), 2012 IEEE 37th Conference on*, pages 952–955, Oct 2012. 37, 40, 41, 80, 83

[draa] Applicability statement for the routing protocol for low power and lossy networks (rpl) in ami networks. `draft-ietf-roll-applicability-ami-10`. 5, 13, 27

[drab] Overview of existing routing protocols for low power and lossy networks. `http://tools.ietf.org/html/draft-levis-roll-overview-protocols-00`. 23

[drac] Roll applicability statement template draft-ietf-roll-applicability-template-06. `https://tools.ietf.org/html/draft-ietf-roll-applicability-template-06`. 26

[drad] Routing requirements for low power and lossy networks. `http://tools.ietf.org/html/draft-culler-rl2n-routing-reqs-01`. 23

BIBLIOGRAPHY

[DWWB09] M. Dohler, T. Watteyne, T. Winter, and D. Barthel. Routing Requirements for Urban Low-Power and Lossy Networks. RFC 5548 (Informational), May 2009. 26

[EL14] Eur-Lex. Report from the commission benchmarking smart metering deployment in the eu-27 with a focus on electricity, 2014. 3

[G3-] G3-plc overview. 5

[GCB03] Jose A. Gutierrez, Edgar H. Callaway, and Raymond Barrett. *IEEE 802.15.4 Low-Rate Wireless Personal Area Networks: Enabling Wireless Sensor Networks*. IEEE Standards Office, New York, NY, USA, 2003. 15

[GFBK11] S. Gormus, Zhong Fan, Z. Bocus, and P. Kulkarni. Opportunistic communications to improve reliability of ami mesh networks. In *Innovative Smart Grid Technologies (ISGT Europe), 2011 2nd IEEE PES International Conference and Exhibition on*, pages 1–8, Dec 2011. 37, 38, 41

[GFJ+09] Omprakash Gnawali, Rodrigo Fonseca, Kyle Jamieson, David Moss, and Philip Levis. Collection tree protocol. In *Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems*, pages 1–14. ACM, 2009. 24

[GK14] Olfa Gaddour and Anis Koubâa. OF-FL : QoS-Aware Fuzzy Logic Objective Function for the RPL Routing Protocol. pages 365–372, 2014. 37, 38, 41, 42

[GKC+12] O. Gaddour, A. Koubaa, S. Chaudhry, M. Tezeghdanti, R. Chaari, and M. Abid. Simulation and performance evaluation of dag construction with rpl. In *Communications and Networking (ComNet), 2012 Third International Conference on*, pages 1–8, March 2012. 57, 69, 80

[GKPG14] Lixia Guan, Koojana Kuladinithi, Thomas Potsch, and Carmelita Goerg. A deeper understanding of interoperability between tinyrpl and contikirpl. In *Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2014 IEEE Ninth International Conference on*, pages 1–6, April 2014. 37, 38, 40, 80

[GL12] O. Gnawali and P. Levis. The Minimum Rank with Hysteresis Objective Function. RFC 6719 (Proposed Standard), September 2012. 27, 33, 34

[GOEED14] NIST Smart Grid, Cyber-Physical Systems Program Office, Energy, and Engineering Laboratory Environment Division. Nist framework

and roadmap for smart grid interoperability standards, release 3.0, 2014. 3

[GSW10] Stefano Galli, Anna Scaglione, and Zhifang Wang. For the grid and through the grid: The role of power line communications in the smart grid. *CoRR*, abs/1010.1973, 2010. 11, 12

[HAN] Wired han characterization campaign - test report. `https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/184798/TR_LAN12AF093-EnergyUK-HAN_PLC_Characterization_test_campaign_Ed03__2_.pdf`. 63

[HC11] Ulrich Herberg and Thomas Clausen. A comparative performance study of the routing protocols load and rpl with bi-directional traffic in low-power and lossy networks (lln). In *Proceedings of the 8th ACM Symposium on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks*, PE-WASUN '11, New York, NY, USA, 2011. ACM. 57, 58

[HM13] Karel Heurtefeux and Hamid Menouar. Experimental evaluation of a routing protocol for wireless sensor networks: RPL under study. *6th Joint IFIP Wireless and Mobile Networking Conference (WMNC)*, pages 1–4, April 2013. 37, 38, 40

[IA13] Gopalakrishnan Iyer and Prathima Agrawal. Performance comparison of Routing Protocols over Smart Utility Networks : A Simulation Study. pages 969–973, 2013. 37, 39, 40

[IEE10] P1901.2 - electrical network and topology channel and noise model-measurements and test results. IEEE Project, September 2010. 3, 4, 14, 15, 19, 20, 105

[ITN13] Oana Iova, Fabrice Theoleyre, and Thomas Noel. Stability and efficiency of RPL under realistic conditions in Wireless Sensor Networks. *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pages 2098–2102, September 2013. 37, 38, 40, 83

[KG11] H.R. Kermajani and C. Gomez. Route change latency in low-power and lossy wireless networks using rpl and 6lowpan neighbor discovery. In *Computers and Communications (ISCC), 2011 IEEE Symposium on*, pages 937–942, June 2011. 80

[LCH+11] P. Levis, T. Clausen, J. Hui, O. Gnawali, and J. Ko. The Trickle Algorithm. RFC 6206 (Proposed Standard), March 2011. 27, 31

[LHG13] Chi-Anh La, Martin Heusse, and Andrzej Duda Grenoble. Link reversal and reactive routing in Low Power and Lossy Networks. *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pages 3386–3390, September 2013. 37, 40

[LOAa] 6lowpan ad hoc on-demand distance vector routing (load). `http://tools.ietf.org/html/draft-daniel-6lowpan-load-adhoc-routing-03`. 5, 24

[LOAb] The lightweight on-demand ad hoc distance-vector routing protocol - next generation (loadng). `https://tools.ietf.org/html/draft-clausen-lln-loadng-12`. 5, 24

[MKHC07] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler. Transmission of IPv6 Packets over IEEE 802.15.4 Networks. RFC 4944 (Proposed Standard), September 2007. Updated by RFCs 6282, 6775. 26

[MMRV10] J. Martocci, P. De Mil, N. Riou, and W. Vermeylen. Building Automation Routing Requirements in Low-Power and Lossy Networks. RFC 5867 (Informational), June 2010. 26

[NIS] Nist framework and roadmap for smart grid interoperability standards, release 3.0. `http://www.nist.gov/smartgrid/upload/NIST-SP-1108r3.pdf`. 10

[OPOP12] George Oikonomou, Iain Phillips, Email G Oikonomou, and I W Phillips. Stateless Multicast Forwarding with RPL in 6LowPAN Sensor Networks. (March), 2012. 37

[PBRD03] C. Perkins, E. Belding-Royer, and S. Das. Ad hoc On-Demand Distance Vector (AODV) Routing. RFC 3561 (Experimental), July 2003. 22

[PRDK12] Y.-A. Pignolet, I. Rinis, D. Dzung, and A. Karaagac. Heterogeneous multi-interface routing: networking stack and simulator extensions. In *Mobile Adhoc and Sensor Systems (MASS), 2012 IEEE 9th International Conference on*, volume Supplement, pages 1–6, Oct 2012. 36, 37

[PTDP09] K. Pister, P. Thubert, S. Dwars, and T. Phinney. Industrial Routing Requirements in Low-Power and Lossy Networks. RFC 5673 (Informational), October 2009. 26

[RLP+] T. Ropitault, A. Lampropulos, A. Pelov, L. Toutain, R. Vedantham, and P. Chiummiento. Realistic model for narrowband plc for advances

metering infrastructure. In *IEEE SmartGridComm 2013 Symposium*. 5, 46, 59, 80

[RLP+14] T. Ropitault, A. Lampropulos, A. Pelov, L. Toutain, R. Vedantham, and P. Chiummiento. Doing it right 2014; recommendations for rpl in plc-based networks for the smart grid. In *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*, pages 452–457, Nov 2014. 5, 6

[RLP+15] T. Ropitault, A. Lampropulos, A. Pelov, L. Toutain, R. Vedantham, and P. Chiummiento. Optimizing plc networks for the smart grid with a new multi-modulation rpl metric – channel occupancy. In *Smart Grid Communications (SmartGridComm), 2015 IEEE International Conference on*, Nov 2015. 6

[SCT11] Leila Ben Saad, Cedric Chauvenet, and Bernard Tourancheau. Simulation of the rpl routing protocol for ipv6 sensor networks: two cases studies. In *International Conference on Sensor Technologies and Applications SENSORCOMM 2011*. IARIA, 2011. 36, 37, 38

[SS01] Curt Schurgers and Mani B Srivastava. Energy efficient routing in wireless sensor networks. In *Military Communications Conference, 2001. MILCOM 2001. Communications for Network-Centric Operations: Creating the Information Force. IEEE*, volume 1, pages 357–361. IEEE, 2001. 24

[TdO13] J. Tripathi and J.C. de Oliveira. On adaptive timers for improved rpl operation in low-power and lossy sensor networks. In *5 International Conf. on Communication Systems and Networks (COMSNETS)*, 2013. 37, 39, 40, 57, 58, 69, 106

[TDOV10] J. Tripathi, J.C. De Oliveira, and J. P Vasseur. Applicability study of rpl with local repair in smart grid substation networks. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pages 262–267, 2010. 81

[Thu12] P. Thubert. Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL). RFC 6552 (Proposed Standard), March 2012. 27, 32, 49

[TZW12] Chun-Ming Tang, Ying Zhang, and Yu-Ping Wu. The p2p-rpl routing protocol research and implementation in contiki operating system. In *Instrumentation, Measurement, Computer, Communication and Control (IMCCC), 2012 Second International Conference on*, pages 1472–1475, Dec 2012. 80

BIBLIOGRAPHY

[VKP+12] JP. Vasseur, M. Kim, K. Pister, N. Dejean, and D. Barthel. Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks. RFC 6551 (Proposed Standard), March 2012. 27, 34

[VTD13] Malisa Vucinic, Bernard Tourancheau, and Andrzej Duda. Performance comparison of the RPL and LOADng routing protocols in a Home Automation scenario. *2013 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1974–1979, April 2013. 37, 39, 40

[WMRD11] Thomas Watteyne, Antonella Molinaro, Maria Grazia Richichi, and Mischa Dohler. From manet to ietf roll standardization: A paradigm shift in wsn routing protocols. *Communications Surveys & Tutorials, IEEE*, 13(4):688–707, 2011. 23, 24

[WTB+12] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, JP. Vasseur, and R. Alexander. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. RFC 6550 (Proposed Standard), March 2012. 4, 24, 90

[YC13] Jiazi Yi and Thomas Clausen. Evaluation of Routing Protocol for Low Power and Lossy Networks : LOADng and RPL. (Lix):19–24, 2013. 37, 39, 40

[ZD02] M. Zimmermann and K. Dostert. A multipath model for the powerline channel. *IEEE Transactions on Communications*, 50(4):553–559, 2002. 47

Résumé

Le réseau électrique a connu récemment une évolution majeure pour se transformer en un réseau électrique intelligent: le Smart Grid (SG). La bidirectionnalité des communications est au cœur du SG et permet de mettre en œuvre et de prendre en compte un ensemble de nouvelles fonctionnalités.

L'Advanced Metering Infrastructure permet d'assurer l'interconnexion entre utilisateurs et opérateurs électrique à l'aide d'une nouvelle génération de compteur: «les compteurs intelligents». Alors que le déploiement de compteur intelligent a déjà commencé dans le monde, une multitude de choix reste encore à faire concernant leur mise-en-œuvre.

Concernant le medium de communication, le Courant Porteur en Ligne (CPL), utilisant les lignes électriques déjà déployées, semble être la solution idéale pour les opérateurs énergétiques. Le standard P901.2 a été standardisé par l'IEEE pour permettre des communication efficaces au sein du SG. Il préconise l'utilisation du protocole IPv6 mais ne donne aucune indication concernant le protocole de routage à utiliser. Le CPL est un environnement extrême de part sa nature (bruits, faibles débits) et peut-être vu comme un Low Power and Lossy Network (LLN). L'IETF a défini le protocole pro-actif RPL spécifiquement pour les LLN et semble, de ce fait, un bon candidat pour les environnements IEEE P1901.2.

Le but de cette thèse a été d'étudier le comportement de RPL dans le Smart Grid et d'apporter des améliorations spécifiques pour le Smart Grid afin de garantir un fonctionnement optimal de RPL dans ce type d'environnement.

Mots-clés : Protocoles de réseaux d'ordinateurs, Réseaux électriques intelligents, Courants porteurs en ligne (informatique), Simulation par ordinateur -- Logiciels.

Abstract

The power grid has begun a major evolution in the past decade, laying the foundations of what is known as the Smart Grid. The Smart Grid relies on bidirectional communications in order to enable new functionalities.

One of the key components of the Smart Grid is the Advanced Metering Infrastructure that enables the interconnection between users and utilities thanks to a new generation of power meters: the Smart Meter. While Smart Meter deployments have already started worldwide at the instigation of governments, a multitude of choices still remains to be done concerning their technical implementations.

Specifically, Smart Meter networking can be based on Power Line Communication (PLC), which is one of the major networking technologies available to utilities. P1901.2, a narrowband PLC has been standardized by the IEEE for usage in the Smart Grid. However, debates are still open for the routing protocol to use for these new high-density, narrowband PLC networks. PLC, being a harsh environment (low bandwidth, noisy, etc.), has most of the characteristics of a Low power and Lossy Network.

As a result, the protocol RPL, designed specifically for Low power and Lossy Network, is a prime candidate for routing in IEEE P1901.2 networks. The goal of this thesis is to study RPL's behavior in Smart Grid environment and to provide adjustments to its behavior in order to improve the network performance in a narrowband PLC network of Smart Meters.

Keywords : Computer network protocols, Smart power grids, Computer simulation -- Software.

TELECOM Bretagne

n° d'ordre : 2015telb0360

Télécom Bretagne

Technopôle Brest-Iroise - CS 83818 - 29238 Brest Cedex 3

Tél : + 33(0) 29 00 11 11 - Fax : + 33(0) 29 00 10 00